FORTINET
High Performance Network Security

FortiOS™ Handbook - What's New

VERSION 5.6.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, April 27, 2017

FortiOS™ Handbook - What's New

01-560-117003-20170427

Executive Summary

This chapter briefly highlights some of the higher profile new FortiOS 5.6 features.

Security Fabric enhancements

Security Fabric features and functionality continue to evolve. New features include improved performance and integration, a security audit function that finds possible problems with your network and recommends solutions, security fabric dashboard widgets, improved device detection, and the remote login to other FortiGates on the fabric. See New Security Fabric features on page 17.

Security Fabric Audit

The Security Fabric Audit allows you to analyze your Security Fabric deployment to identify potential vulnerabilities and highlight best practices that could be used to improve your network's overall security and performance. See Security Fabric Audit and Fabric Score on page 21.

Re-designed Dashboard

The Dashboard has been enhanced to show more information with greater flexibility and more functionality. See New Dashboard Features on page 28 for details.

NGFW Policy Mode

You can operate your FortiGate in NGFW policy mode to simplify applying Application control and Web Filtering to firewall traffic. See NGFW Policy Mode (371602) on page 44.

Flow-based inspection with profile-based NGFW mode is the default inspection mode in FortiOS 5.6.

Transparent web proxy

In addition to the Explicit Web Proxy, FortiOS now supports a Transparent web proxy. You can use the transparent proxy to apply web authentication to HTTP traffic accepted by a firewall policy. See Transparent web proxy (386474) on page 36.

Controlled failover between wireless controllers

Administrators can now define the role of the primary and secondary controllers on the FortiAP unit, allowing the unit to decide the order in which the FortiAP selects a FortiGate unit and how the FortiAP unit fails over to a backup FortiGate unit if the primary FortiGate Fails. See Controlled failover between wireless controllers on page 55.

FortiView Endpoint Vulnerability chart

A new FortiView chart that tracks vulnerability events detected by the FortiClients running on all devices registered with the FortiGate. See New FortiView Endpoint Vulnerability Scanner chart (378647) on page 48.

FortiClient Profile changes

FortiClient profiles have been re-organized and now use the FortiGate to warn or quarantine endpoints that are not compliant with a FortiClient profile. See FortiClient Profile changes (386267, 375049).

Adding Internet services to firewall policies

Internet service objects can be added to firewall policies instead of destination addresses and services. See Adding Internet services to firewall policies (389951).

Source and destination NAT in a single Firewall policy

Extensions to VIPs support more NAT options and other enhancements. See Combining source and destination NAT in the same policy (388718).

Other highlights

- Application Control is a free service
- Real time logging to FortiAnalyzer and FortiCloud
- Multiple PSK for WPA Personal (393320)
- VXLAN support (289354)
- NP6 Host Protection Engine (HPE) to add protection for DDoS attacks (363398)
- FortiGate Logs can be sent to syslog servers in Common Event Format (CEF) (300128)
- New PPPoE features

TABLE OF CONTENTS

Executive Summary 3
- Security Fabric enhancements 3
- Security Fabric Audit 3
- Re-designed Dashboard 3
- NGFW Policy Mode 3
- Transparent web proxy 3
- Controlled failover between wireless controllers 4
- FortiView Endpoint Vulnerability chart 4
- FortiClient Profile changes 4
- Adding Internet services to firewall policies 4
- Source and destination NAT in a single Firewall policy 4
- Other highlights 4

Change Log 14

Introduction 15
- How this guide is organized 15

New Security Fabric features 17
- Setting up a FortiOS 5.6 Security Fabric 17
- Security Fabric dashboard widgets 17
- Physical/Logical FortiView Improvements 18
- FortiClient Vulnerability Score 18
- FortiView Consolidation 19
- Remote login to downstream FortiGates 19
- Logging Consolidation and Improvements 19
  - Sending all logs to a single FortiAnalyzer 19
  - Data Exchange with FortiAnalyzer 20
  - Retrieving Monitor Information 20
  - Log Settings 20
- Device Tree 20

Security Fabric Audit and Fabric Score 21
- What is the Security Fabric Audit? 21
- Why should you run a Security Fabric Audit? 21
- Running a Security Fabric Audit 21
- Logging for the Security Fabric Audit 23
- Security Fabric Audit Checks 24

Firmware & Subscriptions 24
Internal Segmentation Firewall (ISFW) 24
Endpoint Compliance 25
Security Best Practices 26
Security Fabric Score 26
New Dashboard Features 28
System Information 29
Licenses 30
FortiCloud 31
Security Fabric 31
Administrators 31
CPU 32
Memory 32
Sessions 33
Bandwidth 33
FortiExplorer for iOS 34
Transparent web proxy (386474) 36
Using the Transparent proxy 36
More about the transparent proxy 38
Flat policies 38
Authentication 39
New Proxy Type 39
IP pools support 40
SOCKSv5 40
Forwarding 40
Support for explicit proxy address objects & groups into IPv4 firewall policies 40
Support application service in the proxy based on HTTP requests 40
CLI 41
NGFW Policy Mode (371602) 44
NGFW policy mode and NAT 44
Application control in NGFW policy mode 45
Web Filtering in NGFW mode 46
Other NGFW policy mode options 47
New FortiView Endpoint Vulnerability Scanner chart (378647) 48
FortiClient Profile changes (386267, 375049) 49
Default FortClient profile 49
Endpoint vulnerability scanning 49
System compliance 50
Security posture checking 50
Application Control is a free service 52
IPS / Application Control logging performance 52

Real time logging to FortiAnalyzer and FortiCloud 53
Reliable Logging updated for real-time functionality (378937) 53
FortiGate Logs can be sent to syslog servers in Common Event Format (CEF) (300128) 54
Controlled failover between wireless controllers 55
1+1 Wireless Controller HA 55
Primary and secondary ACs 55
1+1 redundancy 55
Multiple PSK for WPA Personal (393320) 56
VXLAN support (289354) 57
VTEP (VXLAN Tunnel End Point) support (289354) 57
VXLAN support for multiple remote IPs (398959) 58
New PPPoE features 59
PPPoE dynamic gateway support (397628) 59
Support multiple PPPoE connections on a single interface (363958) 59
Adding Internet services to firewall policies (389951) 62
CLI 62
GUI 62
Combining source and destination NAT in the same policy (388718) 63
NP6 Host Protection Engine (HPE) to add protection for DDoS attacks (363398) 65
New feature catalog 67
Authentication 68
FortiToken Mobile Push (397912, 408273, 399839, 404872) 68
Support V4 BIOS certificate (392960) 68
Support extendedKeyUsage for x.509 certificates (390393) 69
Administrator name added to system event log (386395) 69
Support RSA-4096 bit key-length generation (380278) 69
New commands added to config user ldap to set UPN processing method and filter name (383561) 69
User authentication max timeout setting change (378085) 70
Changes to Authentication Settings > Certificates GUI (374980) 70
Password for private key configurable in both GUI and CLI (374593) 70
RADIUS password encoding (365145) 70
RSSO supports Delegated-IPv6-Prefix and Framed-IPv6-Prefix (290990) 70
Device identification 71
Changed default for device-identification-active-scan to disabled (380837) 71
Diagnose command changes 72
Add missing "diag npu np6 ..." Commands (305808) 72
Diagnose command to show firewall service cache (355819) 72
Diagnose command to show crash history and adjust crash interval (366691) 73

diagnose switch-controller commands (368197) 73
Diagnose commands for monitoring NAT sessions (376546) 74
SIP diagnose command improvements (376853) 75
Diagnose command to get AV virus statistics (378870) 76
Diagnose command to get remote FortiSwitch trunk information (379329) 76
help provided for diagnose debug application csfd (379675) 77
New IPS engine diagnose commands (381371) 77
New AV engine diagnose commands (383352) 78
NPU diagnose command now included HPE info in results (384692) 78
clear checksum log files (diag sys ha checksum log clear) (385905) 78
new diagnose command to delete avatars (388634) 79
CID signatures have been improved for DHCP and CDP (389350, 409436) 79
diagnose command to calculate socket memory usage (392655) 79
FortiGuard can determine a FortiGate's location from its public IP address (393972) 80
AWS bootstrapping diagnose commands (394158) 81
Diagnose command to aid in conserver mode issues (394856) 81
Diagnose commands to display FortiCare registration information (395254) 81
new diag test app csfd options (395302) 82
new 'AND' and 'OR' filter capabilities for debug flow addr (398985) 83
Improve wad debug trace and crash log information (400454) 83
diag sys sip-proxy config profile --> diag sys sip-proxy config profiles (404874) 83
diag debug flow changes (405348) 83
improve wad memory diagnose process (408236) 83
New daemon watchdog framework in forticron (409243) 84
DNS log improvements (410132) 84
Explicit web proxy 85
Explicit proxy supports multiple incoming ports and port ranges (402775, 398687) 85
Explicit proxy supports IP pools (402221) 85
Option to remove unsupported encoding from HTTP headers (392908) 85
New authentication process for explicit web proxying (386474, 404355) 85
Added Internet services to explicit proxy policies (386182) 86
Virtual WAN link in an explicit proxy firewall policy (385849, 396780) 86
Added application ID and category setting on the explicit proxy enabled service (379330) 86
Explicit Proxy - populate pac-file-url in transparent mode (373977) 86
SSL deep inspection OCSP support for Explicit Proxy (365843) 87
Timed out authentication requests are now logged (357098) 87
Firewall 88
Optimization of the firewall Service cache (355819) 88
New CLI option to prevent packet order problems for sessions offloaded to NP4 or NP6 (365497) 88
GUI changes to Central NAT (371516) 88

Max value for Firewall User authentication changed (378085) 88
Changes to default SSL inspection configuration (380736) 89
Add firewall policy comment field content to log messages (387865) 89
Learning mode changes profile type to single (387999) 90
MAC address authentication in firewall policies and captive portals (391739) 90
Display resolved IP addresses for FQDN in policy list (393927) 90
Added comment for acl-policy, interface-policy and DoS-policy (396569) 90
Internet service settings moved to more logical place in CLI (397029) 91
Certificate key size selection (397883) 93
AWS API integration for dynamic firewall address object (400265) 93
Internet service configuration (405518) 94
Changes to SSL abbreviate handshake (407544) 95
NGFW mode in the VDOM - NAT & SSL Inspection considerations (407547) 95
Managed FortiSwitch 98
Aggregating FortiSwitches into groups (397950) 98
Pre-authentication and Replacements of FortiSwitches (298533) 98
LLDP MED on Managed FortiSwitches (372288) 98
Enhanced 802.1x including FortiSwitch port security policy framework (389102) 99
Firmware upgrade management and compatible version information (385171) 100
Changed Managed-Switch Display Format for 'dynamic-capability' (387239) 100
Connecting to a managed switch CLI from the FortiGate GUI (378119) 101
Firmware upgrade of stacked or tiered switches (355050) 101
More information displayed by the execute switch-controller get-conn-status command (388751) 101
User-port Link Aggregation Groups available on the GUI (378470) 101
DHCP blocking, STP and Loop Guard on Managed FortiSwitch ports on the GUI (375860) 102
New Switch Profiles (387398) 102
Miscellanous configuration option changes 103
FortiView 103
Added Vulnerability score topology view (303786) 103
FortiView VPN tunnel map feature (382767) 103
Updated FortiView CSF topology pages (384188) 103
Historical FortiView includes FortiAnalyzer (387423) 103
FortiView menu reorganization (399713) 103
Data Exchange with FortiAnalyzer (393891) 104
Google Maps Integration 104
FortiView usability and organization updates (306247) 104
FortiGate VM 105
FGT-VM VCPUs (308297) 105
Improvements to License page (382128) 105
Citrix XenServer tools support for XenServer VMs (387984) 105

FOS VM supports more interfaces (393068) 106
NSX security group importing (403975) 106
Non-vdom VM models FGVM1V/FGVM2V/FGVM4V (405549) 106
Hardware acceleration 108
Improved visibility of SPU and nTurbo hardware acceleration (389711) 108
NP4Lite option to disable offloading ICMP traffic in IPsec tunnels (383939) 108
NP6 IPv4 invalid checksum anomaly checking (387675) 108
High Availability 110
Multicast session failover (293751) 110
Performance improvement when shutting down or rebooting the primary unit (380279) 110
VRRP failover process change (390938) 110
Display cluster up time and history (get system ha status command changes)(394745) 111
In-band HA management Interface (401378) 111
Up to four dedicated HA management interfaces supported (378127) 111
FGSP support for automatic session sync after peer reboot (365851) 112
Change in cluster behavior when the primary unit is restarted (380279) 112
IPsec VPN 113
Improvement to stats crypto command output (403995) 113
Improved certificate key size control commands (397883) 113
Support bit-based keys in IKE (397712) 113
IKEv2 asymmetric authentication (393073) 113
Allow mode-cfg with childless IKEv2 (391567) 114
IKEv2 Digital Signature Authentication support (389001) 114
Passive static IPsec VPN (387913) 114
Phase 2 wizard simplified (387725) 114
Unique IKE ID enforcement (383296) 115
FortiView VPN tunnel map feature (382767) 115
Childless IKEv2 initiation (381650) 115
Allow peertype dialup for IKEv2 pre-shared key dynamic phase1 (378714) 116
IPsec default phase1/phase1-interface peertype changed from 'any' to 'peer' (376340) 116
IPsec GUI bug fixes (374326) 116
Support for IKEv2 Message Fragmentation (371241) 116
IPsec monitoring pages now based on phase 1 proposals not phase 2 (304246) 117
IPv6 118
FortiGate can reply to an anycast probe from the interface’s unicast address (308872) 118
Secure Neighbor Discovery (355946) 118
Add multicast-PMTU to allow FGT to send ICMPv6 Too Big Message (373396) 119
Logging and Reporting 121
Client and server certificates included in Application control log messages (406203) 121
DNS Logging (401757) 121

Added Policy Comment logging option (387865) 121
FortiAnalyzer encryption option name change (399191) 121
Networking 122
New command to get transceiver signal strength (205138) 122
New BGP local-AS support (307530) 122
Interface setting removed from SNMP community (310665) 122
RPF checks can be removed from the state evaluation process (311005) 123
BGP graceful-restart-end-on-timer, stale-route, and linkdown-failover options (374140) 123
FQDNs can be destination addresses in static routes (376200) 123
Priority for Blackhole routes (378232) 124
New DDNS refresh interval (383994) 124
Support IPv6 blackhole routes on GUI (388599) 124
SSL-VPN can use a WAN link load balancing interface (396236) 125
DDNS support for noip.com (399126) 125
IPv6 Router Advertisement options for DNS (399406) 125
WAN LLB to SD-WAN on GUI (403102) 126
RFCs supported by FortiOS 5.6 127
Security Profiles 128
New FortiGuard Web Filter categories (407574) 128
Overall improvement to SSL inspection performance (405224) 128
FortiClient Endpoint license updates (401721) 128
FortiClient Vulnerability Exemption Setting (407230) 129
DNS profile supports safe search (403275) 129
Application control and Industrial signatures separate from IPS signatures (382053) 130
Changes to default SSL inspection configuration (380736) 130
Block Google QUIC protocol in default Application Control configuration (385190) 131
Botnet database changes (390756) 131
Security Fabric audit check for endpoint vulnerability and unauthorized FAP and FSW (401462) 131
Change to CLI commands for configuring custom Internet services (397029) 131
Enable "sync-session-ttl" in "config ips global" CLI by default (399737) 132
CASI functionality moved into application control (385183 372103) 133
New diagnose command to delete avatars (388634) 133
Fortinet bar option disabled in profile protocol options when VDOM is in flow-based inspection mode (384953) 133
SSL/SSH profile certificate handling changes (373835) 134
Restricting access to YouTube (replacement for the YouTube Education filter feature) (378277) 134
Enhancements to IPS Signatures page (285543) 134
DLP sensor GUI changes (307225) 134
Web Filter profile page GUI updates (309012) 134
Web Filter Quota traffic can no longer be set to 0 (374380) 135

Webcache-https and SSL deep inspection profile configuration changes (381101) 135
FortiGate conserve mode changes (242562, 386503) 135
New custom IPS and Application Control Signatures list (280954) 135
Server Load balancing 137
IPv6, 6to4, and 4to6 server load balancing (280073) 137
Improved Server load balancing GUI pages (404169) 137
SSL VPN 138
Remote desktop configuration changes (410648) 138
SSL VPN supports WAN link load balancing interface (396236) 138
SSL VPN login timeout to support high latency (394583) 138
SSL VPN supports Windows 10 OS check (387276) 139
SSL VPN DNS suffix per portal and number of portals (383754) 139
New SSL VPN timeout settings (379870) 139
Personal bookmark improvements (377500) 140
New controls for SSL VPN client login limits (376983) 140
Unrated category removed from ssl-exempt (356428) 140
Clipboard support for SSL VPN remote desktop connections (307465) 140
System 141
Remove CLI commands from 1-CPU platforms (405321) 141
New SNMP trap for bypass events (307329) 141
Implement SNMP support for NAT Session monitoring which includes new SNMP OIDs (383661) 141
New extended database version OIDs for AV and IPS (402162) 141
Administrator password encryption hash upgraded from SHA1 to SHA256 (391576) 141
Allow multiple FortiManager addresses when configuring central management (388083) 142
FortiGuard can determine a FortiGate's location from its public IP address (393972) 142
Deletion of multiple saved configurations supported (308936) 142
New CLI option to limit script output size (388221) 142
Enable / disable logging of SSL connection events (375582) 142
Enabling or disabling static key ciphers (379616) 143
Enhancements to IPS Signatures page (285543) 143
Combine multiple commands into a CLI alias (308921) 143
VoIP/SIP 144
SIP strict-register enabled by default in VoIP Profiles (380830) 144
SIP diagnose command improvements (376853) 144
WiFi 146
Captive Portal Authentication with FortiAP in Bridge Mode (408915) 146
802.11kv(r) support (405498, 395037) 146
External Captive Portal authentication with FortiAP in Bridge Mode (403115, 384872) 146
Japan DFS support for FAP-421E/423E/S421E/S423E (402287, 401434) 147
802.3az support on WAVE2 WiFi APs (400558) 147

CLI command update made in wids-profile (400263) 147
Channel utilization, FortiPresence support on AP mode, QoS enhancement for voice (399134, 377562) 147
FAP-U421E and FAP-U423E support (397900) 148
Minor reorganization of WiFi GUI entries (396497) 149
Multiple PSK support for WPA personal (393320, 264744) 149
Table size of qos-profile has VDOM limit (388070) 149
Add "dhcp-lease-time" setting to local-standalone-nat VAP (384229) 150
New CLI command to configure LDPC for FortiAP (383864) 150
New region code/SKU for Indonesia (382926) 150
FortiAP RMA support added (381936) 150
Support fixed-length 64-hex digit for WPA-Personal passphrase (381030) 150
Allow FortiGates to manage cloud-based FortiAPs (380150) 151
Use IPsec instead of DTLS to protect CAPWAP tunnels (379502) 151
New option added to support only one IP per one endpoint association (378207) 151
FAP-222C-K DFS support (377795) 151
Dynamic VLAN support in standalone mode (377298) 152
CLI-only features added to GUI (376891) 152
Managed AP GUI update (375376) 152
Bonjour gateway support (373659) 152
FAP421E/423E wave2 support (371374) 153
WiFi Health Monitor GUI changes (308317) 153
AP Profile GUI page updates (298266) 153
N+1 Wireless Controller HA (294656) 153
Support for duplicate SSID names on tunnel and bridge mode interfaces (278955) 154
Controlled failover between wireless controllers (249515) 154

Change Log

Date	Change Description
April 27, 2017	Correction to the information about FortiAnalyzer dependency of the Security Fabric in New Security Fabric features on page 17.
April 12, 2017	Updated information on the FortiExplorer iOS app. Updated NGFW Policy Mode (371602) on page 44 to mention that Flow-based is the default inspection mode for FortiOS 5.6. Corrected the CLI alias section in System on page 141.
April 7, 2017	Misc edits and fixes throughout the document.
March 31, 2017	Fixes to FortiExplorer for iOS on page 34.
March 30, 2017	First version.

Introduction

This document highlights and describes many of the new features in FortiOS 5.6. Most new feature descriptions include a feature number that references the internal Fortinet ID used to track the feature.

How this guide is organized

The following sections highlight some of the higher profile new FortiOS 5.6 features.

- New Dashboard Features
- New Security Fabric features
- Security Fabric Audit and Fabric Score
- FortiExplorer for iOS
- NGFW Policy Mode (371602)
- Transparent web proxy (386474)
- New FortiView Endpoint Vulnerability Scanner chart (378647)
- FortiClient Profile changes (386267, 375049)
- Application Control is a free service
- Real time logging to FortiAnalyzer and FortiCloud
- FortiGate Logs can be sent to syslog servers in Common Event Format (CEF) (300128)
- Controlled failover between wireless controllers
- Multiple PSK for WPA Personal (393320)
- VXLAN support (289354)
- New PPPoE features
- Adding Internet services to firewall policies (389951)
- Combining source and destination NAT in the same policy (388718)
- NP6 Host Protection Engine (HPE) to add protection for DDoS attacks (363398)

All of the other new features in FortiOS 5.6 are organized alphabetically by subject:

- Authentication
- Device identification
- Diagnose command changes
- Explicit web proxy
- Firewall
- Managed FortiSwitch
- FortiView
- FortiGate VM
- Hardware acceleration
- High Availability
- IPsec VPN
- IPv6

- Logging and Reporting
- Networking
- RFCs supported by FortiOS 5.6
- Security Profiles
- Server Load balancing
- SSL VPN
- System
- VoIP/SIP
- WiFi

New Security Fabric features

In FortiOS 5.6, the Security Fabric (previously known Cooperative Security Fabric) has been expanded on in several ways to add more functionality and visibility.

One of the most important functional change is that FortiAnalyzer is now a required part of a Security Fabric configuration. Also, two important new features, Security Fabric Audit and Fabric Score, have been added to provide a method to continually monitor and improve Security Fabric's configuration.

Many changes have been made through FortiView to improve Fabric visibility. More information is now displayed and you can access downstream FortiGates directly from the root FortiGate's FortiView display.

Other smaller improvements have been made throughout the Fabric, with a focus on improving communication between devices.

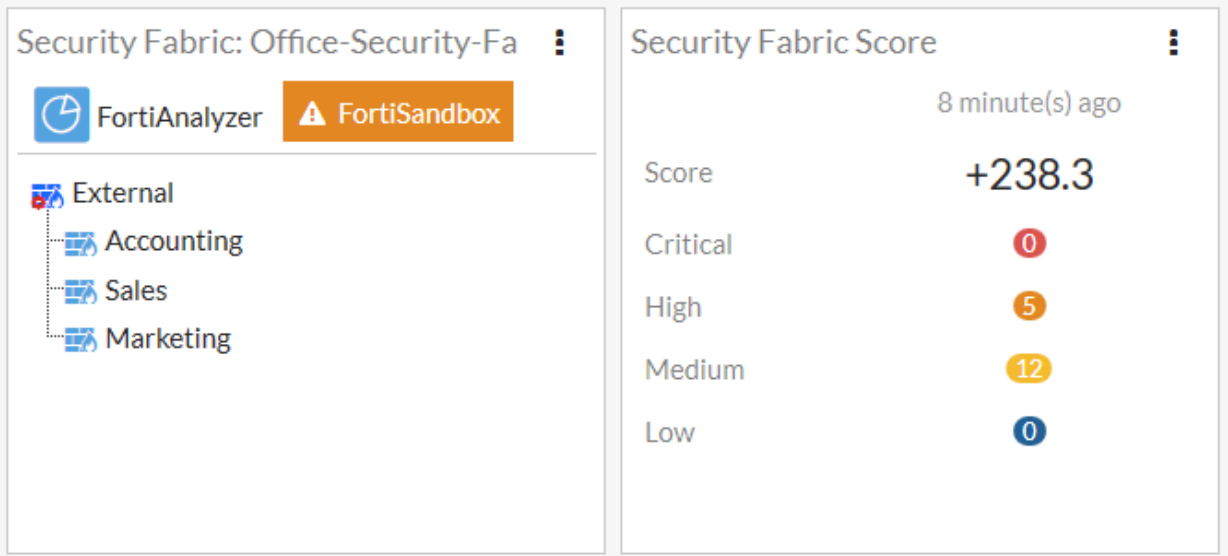
Setting up a FortiOS 5.6 Security Fabric

See the following cookbook recipes to get started setting up a FortiOS 5.6 Security Fabric:

- Installing a FortiGate in NAT/Route mode
- Security Fabric installation

Security Fabric dashboard widgets

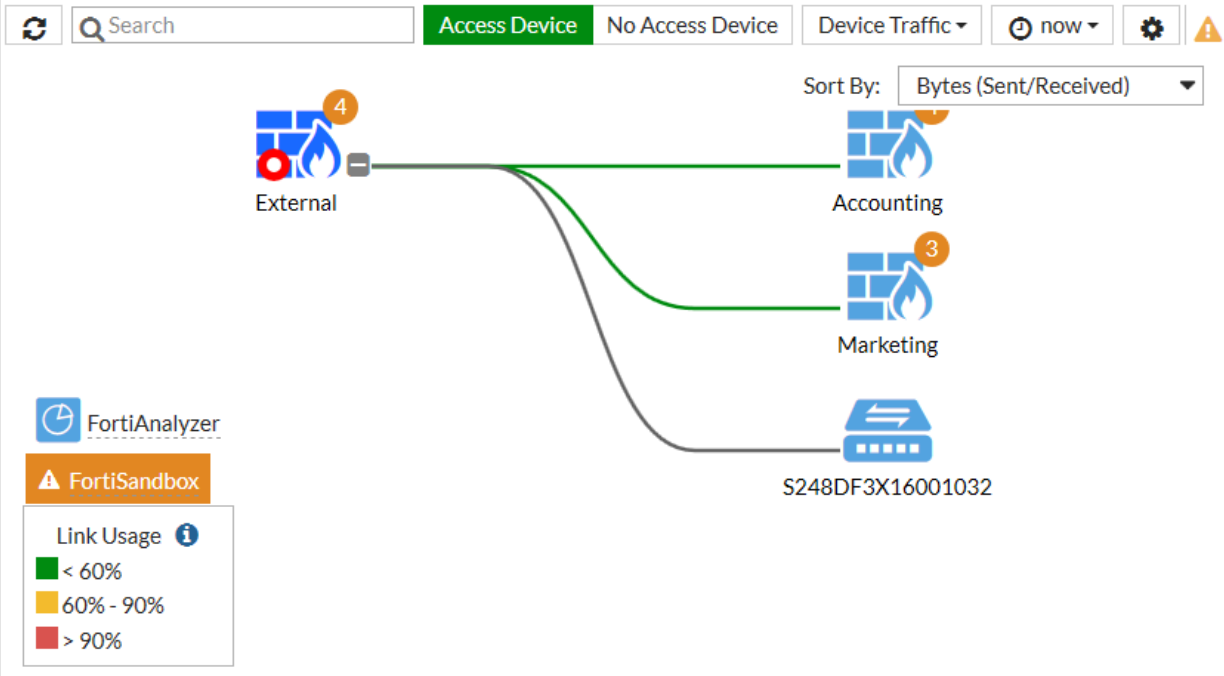
New security fabric dashboard widgets put security fabric status information at your fingertips when you first log into your FortiGate.



Physical/Logical FortiView Improvements

The FortiView Physical and Logical topology pages now display the following:

- Both FortiGates in an HA configuration
- FortiAPs
- FortiAnalyzer and FortiSandbox are listed as fabric components
- The current FortiGate is highlighted
- Link Usage is displayed with different colors
- Endpoints ranked by FortiClient Vulnerability Score and by Threat Score (for more info, see below)
- User avatars
- Servers are now a recognized device type
- A search bar is now available to help locate specific devices in the Security Fabric.



FortiClient Vulnerability Score

Endpoints in the Security Fabric topology are now ranked by their FortiClient Vulnerability Score. This score is calculated by the severity of vulnerabilities found on the endpoint:

- critical vulnerability = 100 points
- high vulnerability = 50 points
- medium vulnerability = 5 points

- low vulnerability = 2 points
- info vulnerability = 1 point

FortiView Consolidation

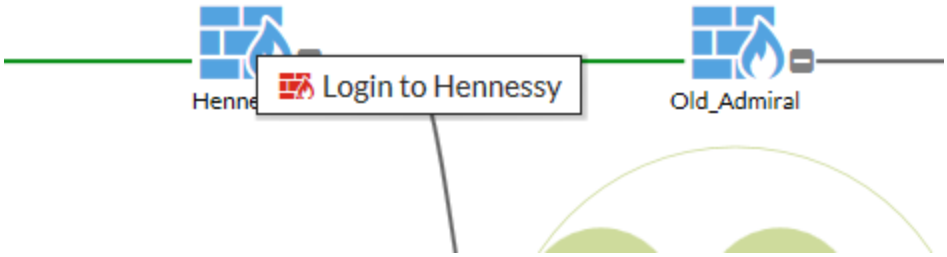
Information about a security fabric can now be seen throughout the FortiView dashboards on the upstream FortiGate, when the realtime view is used.

- You can right-click on an entry and select View Aggregated Details to see more information.
- The upstream FortiGate filters information to avoid counting traffic from the same hosts multiple times on each hop.

The upstream FortiGate also now has the option to end downstream FortiGate sessions or quarantine endpoints that connect to downstream FortiGates.

Remote login to downstream FortiGates

You can now log into downstream FortiGates from the upstream FortiGate, by right-clicking on the downstream FortiGate when viewing the Security Fabric's topology using FortiView.



Logging Consolidation and Improvements

Several changes have been made to improve logging for a Security Fabric.

Sending all logs to a single FortiAnalyzer

By default, all FortiGates in a Security Fabric now send logs to a single FortiAnalyzer. The connection to the FortiAnalyzer is configured on the upstream FortiGate, then the settings are pushed to all other FortiGates.

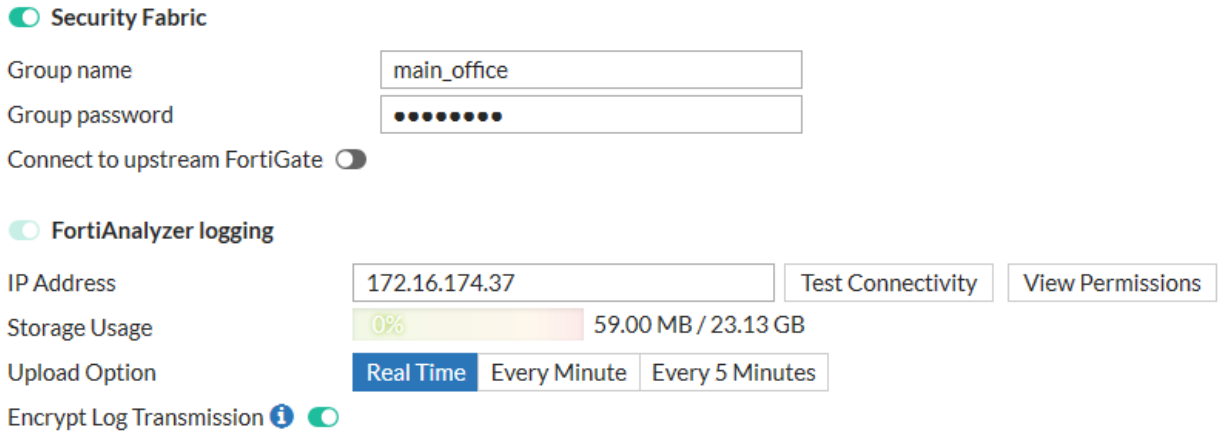
In FortiOS 5.6, a FortiAanlyzer is required for the root FortiGate in a Security Fabric; however, downstream devices can be configured to use other logging methods through the CLI:

```
config system csf
   set logging-mode local
end
```

Data Exchange with FortiAnalyzer

The following information about the Security Fabric configuration is now sent to the FortiAnalyzer:

- Topology info
- Interface roles
- LAT / LNG info
- Device asset tags



Retrieving Monitor Information

Monitors on the upstream FortiGate, such as the VPN Monitor, Route Monitor, and User Quarantine, can now view the info from downstream devices. You can use the button on the top right corner of the screen to change with FortiGate's information is displayed.

Log Settings

Log statistics for each FortiGate in the Security Fabric are now shown when you go to **Log & Report > Log Settings**.

Device Tree

The whole Security Fabric tree is now updated upward and each node has updated state of the whole subtree. The content is saved in the local file and upon request from the GUI or a diagnose command (dia sys csf downstream) it can be retrieved.

Security Fabric Audit and Fabric Score

This chapter contains information about the Security Fabric Audit and Fabric Score, which together provide a method to continually monitor and improve your Security Fabric's configuration.

What is the Security Fabric Audit?

The Security Fabric Audit is a feature on your FortiGate that allows you to analyze your Security Fabric deployment to identify potential vulnerabilities and highlight best practices that could be used to improve your network's overall security and performance.

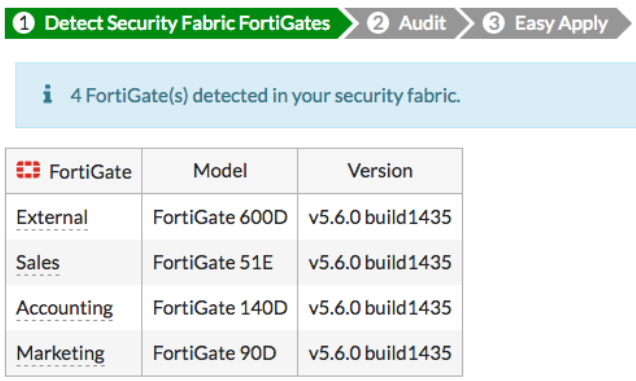
Why should you run a Security Fabric Audit?

Using the Security Fabric Audit helps you to tune your network's configuration, deploy new hardware and/or software, and gain more visibility and control of your network. Also, by checking your Security Fabric Score, which is determined based on how many checks your network passes/fails during the Audit, you can have confidence that your network is getting more secure over time.

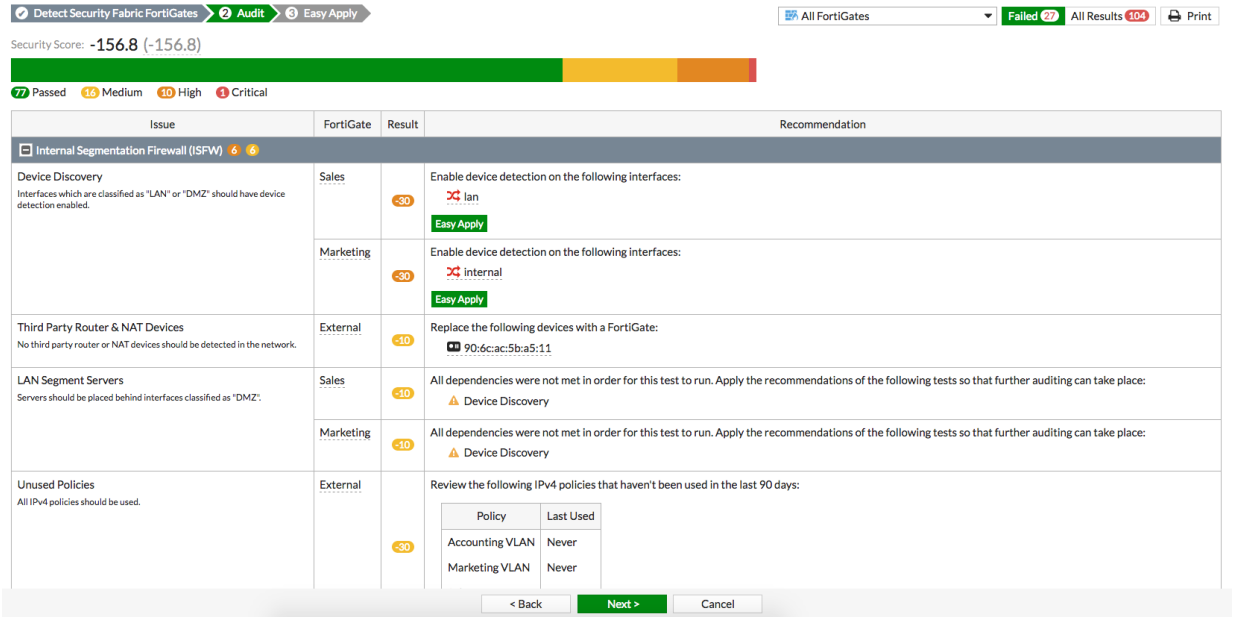
Running a Security Fabric Audit

The Security Fabric Audit must be run on the root FortiGate in the Security Fabric.

The Security Fabric Audit can be found by going to **Log & Report > Security Fabric Audit**. In the first step, all detected FortiGates are shown.

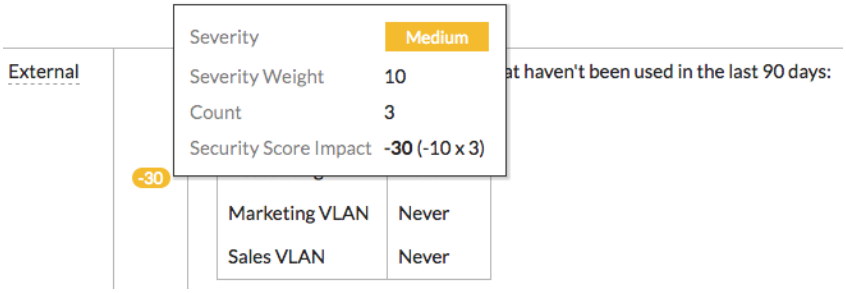


In the second step, the audit is performed and a list of recommendations are shown. Two views are available: **Failed** or **All Results**. These views can be further segmented so that you view results from all FortiGates or just a specific unit.



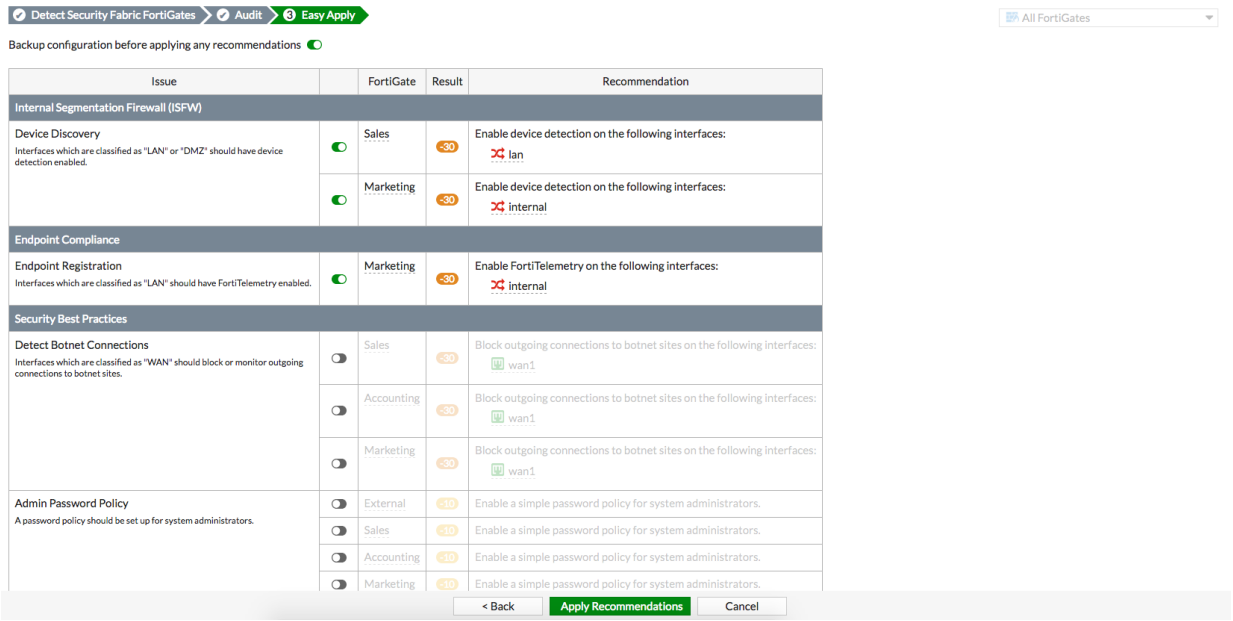
In each view, a chart appears showing the results of individual checks. The following information is shown: the name and a description of the check, which FortiGate the check occurred on, the checks result on your overall security score, and any necessary recommendations.

If you hover the mouse over the **Result** for a check, you can get a breakdown on how this score was determined. For more information about this, see "Security Fabric Score" on page 26.

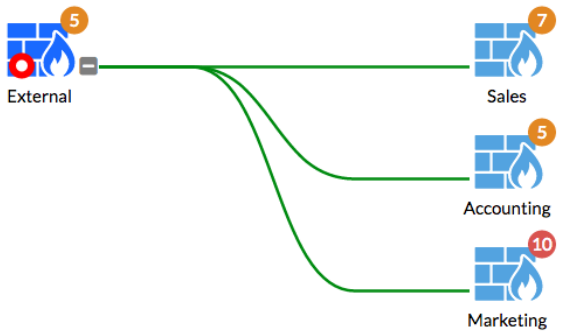


In Step Three of the Audit, **Easy Apply** recommendations are displayed and can be applied. By using **Easy Apply**, you can change the configuration of any FortiGate in the fabric.

For other recommendations, further action is required if you wish to follow the recommendation.



You can also view Audit recommendations for specific devices using the FortiView Topology consoles. If a recommendation is available for a device, a circle containing a number appears. The number shows how many recommendations are available, while the color of the circle shows the severity of the highest check that failed (red is critical, orange is high, yellow is medium, and blue is low).



Logging for the Security Fabric Audit

An event filter subtype is available for the Security Audit. Every time an audit is run, event logs are created on the root FortiGate that summarize the results of the audit, as well as details into the individual tests.

Syntax

```
config log eventfilter
      set security-audit {enable | disable} (enabled by default)
end
```

Security Fabric Audit Checks

The Security Fabric Audit performs a variety of checks when analyzing your network. All checks are based on your current network configuration, using realtime monitoring. The Audit runs these checks across all FortiGates in the Security Fabric.

Firmware & Subscriptions

Goal	Severity	Check	Recommendation	Easy Apply?
Compatible Firmware	Critical	All FortiGates in the Security Fabric should run the same firmware version.	Run same version as root.	No
FortiCare Support	Critical	FortiGate should be registered with FortiCare.	Register with FortiCare.	No
FortiGuard License Subscriptions	High	All registered FortiGuard license subscriptions should be valid.	Renew subscriptions.	No
FortiAP Firmware Versions	Low	All FortiAPs should be running the latest firmware.	Upgrade FortiAP to recommended version.	No
FortiSwitch Firmware Versions	Low	All FortiSwitches should be running the latest firmware.	Update all FortiSwitches to use the latest firmware.	No

Internal Segmentation Firewall (ISFW)

Goal	Severity	Check	Recommendation	Easy Apply?
Interface Classification	High	All interfaces should be classified as either "LAN", "WAN", or "DMZ".	Configure the interface role.	Yes
Device Discovery	High	Interfaces which are classified as "LAN" or "DMZ" should have device detection enabled.	Enable device detection.	Yes
Third Party Router & NAT Devices	Medium	No third party router or NAT devices should be detected in the network.	Replace the device with a FortiGate.	No
VLAN Management	Medium	Non-FortiLink interfaces should not have multiple VLANs configured on them.	Use FortiSwitch and FortiLink.	No

Goal	Severity	Check	Recommendation	Easy Apply?
Centralized Logging & Reporting	High	Logging and reporting should be done in a centralized place throughout the Security Fabric.	Install FortiAnalyzer for logging & reporting.	No
LAN Segment	Medium	Servers should be placed behind interfaces classified as "DMZ".	All servers should be moved to interfaces with role "DMZ".	No
Unused Policies	Medium	All IPv4 policies should be used.	Review all IPv4 policies that haven't been used in the last 90 days.	No
Advanced Threat Protection	High	Suspicious files should be submitted to FortiSandbox or FortiSandbox Cloud for inspection.	Configure AntiVirus profiles to send files to FortiSandbox or FortiSandbox Cloud for inspection.	No
Unauthorized FortiAPs	Medium	All discovered FortiAPs should be authorized or disabled.	Authorize or disable unauthorized FortiAPs.	Yes
Unauthorized FortiSwitches	Medium	All discovered FortiSwitches should be authorized or disabled.	Authorize or disable unauthorized FortiSwitches.	Yes

Endpoint Compliance

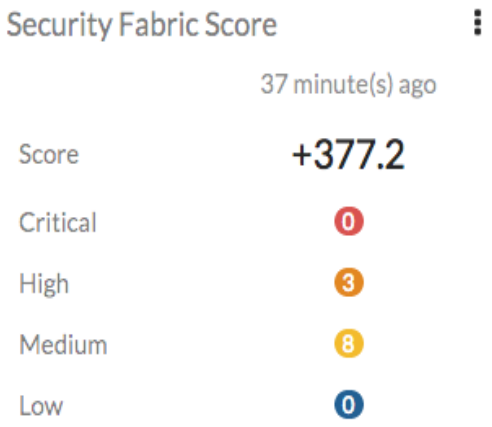
Goal	Severity	Check	Recommendation	Easy Apply?
Endpoint Registration	High	Interfaces which are classified as "LAN" should have FortiTelemetry enabled.	Enable FortiTelemetry on "LAN" interfaces.	Yes
FortiClient Protected	Medium	All supported devices should be registered via FortiClient.	Register all devices via FortiClient.	No
FortiClient Compliance	Medium	All registered FortiClient devices should be compliant with FortiClient profile.	Investigate non-compliant reason(s) for FortiClient endpoints.	No
FortiClient Vulnerabilities	Critical	All registered FortiClient devices should have no critical vulnerabilities.	Have FortiClient fix the detected critical vulnerabilities.	No

Security Best Practices

Goal	Severity	Check	Recommendation	Easy Apply?
Detect Botnet Connections	High	Interfaces which are classified as "WAN" should block or monitor outgoing connections to botnet sites	Enable botnet detection on “WAN” interfaces.	Yes
Unsecure Protocol - HTTP	High	Interfaces which are classified as "WAN" should not allow HTTP administrative access.	Enable HTTPS redirection globally.	Yes
Unsecure Protocol - Telnet	High	Interfaces which are classified as "WAN" should not allow Telnet administrative access.	Disable Telnet.	Yes
Valid HTTPS Certificate - Administrative GUI	Medium	The administrative GUI should not be using a default built-in certificate.	Acquire a certificate for your domain, upload it, and configure the administrative GUI to use it.	No
Valid HTTPS Certificate - SSL VPN	Medium	SSL VPN should not be using a default built-in certificate.	Acquire a certificate for your domain, upload it, and configure SSL VPN to use it.	No
Explicit Interface Policies	Low	Policies that allow traffic should not be using the "any" interface.	Change the policy to use a specific interface.	No
Admin Password Policy	Medium	A password policy should be setup for system administrators.	Enable a simple password policy for system administrators.	Yes

Security Fabric Score

The **Security Fabric Score** widget has been added to the FortiGate Dashboard to give visibility into auditing trends. This widget uses information from the Security Fabric Audit to determine your score. Score can be positive or negative, with a higher score representing a more secure network.



Score is based on the number of checks failed and the severity of these checks. The weight for each severity level is as follows:

- Critical: 50 points
- High: 25 points
- Medium: 10 points
- Low: 5 points

You get points for passing a test only when it passes for all FortiGates in your fabric. If this occurs, the score is calculated using this formula:

+Severity Weight x Secure FortiGate Multiplier

The Severity Weight is calculated as Severity divided by the number of FortiGates in the Fabric. The Secure FortiGate Multiplier is determined using logarithms and the number of FortiGates in the fabric. For example, if you have four FortiGates in your fabric that all pass the Compatible Firmware check, your score for each individual FortiGate is:

(50/4) x 1.292 = 16.2 points

If a test fails on any FortiGate in your Fabric, all other FortiGates that passed the check award 0 points. For the FortiGate the test failed on, the score is calculated using this formula:

-Severity Weight x Count

Count is the number of times the check failed during the audit. For example, if two critical FortiClient vulnerabilities are discovered during the Audit, your score for that check is:

-50 x 2 = -100 points

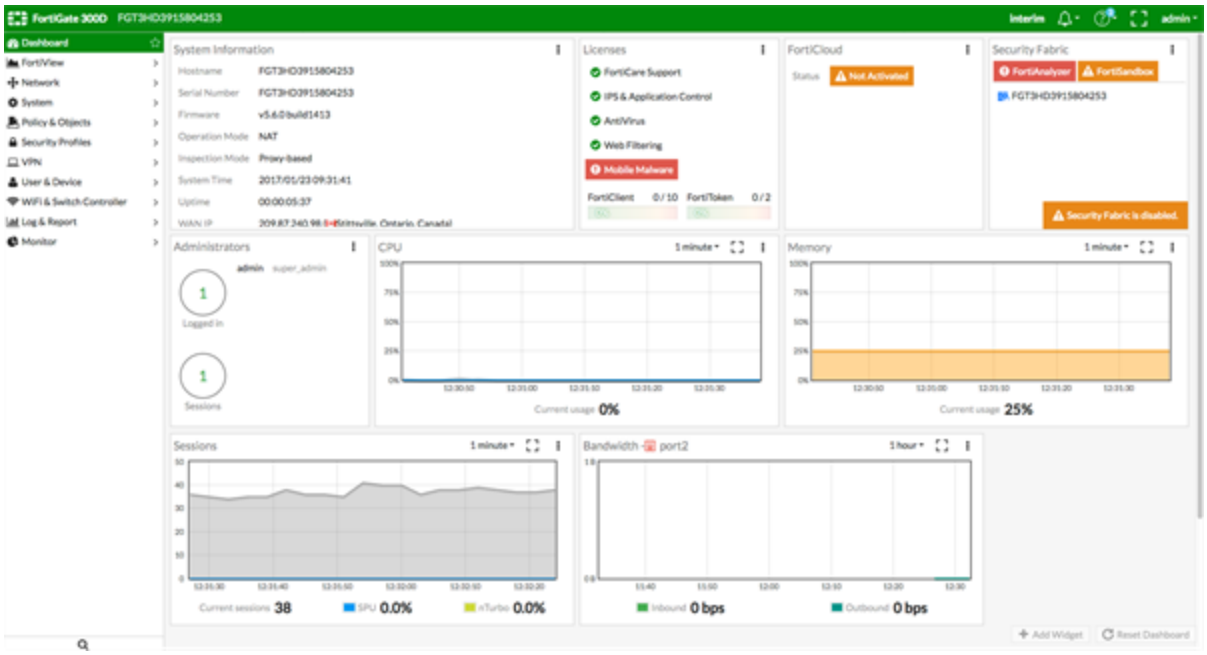
For checks that do not apply, your score does not change. For example, if you have no FortiAPs in the fabric, you will receive no points for the FortiAP Firmware Versions check.

New Dashboard Features

The FortiOS 5.6 **Dashboard** has a new layout with a Network Operations Center (NOC) view with a focus on alerts. Widgets are interactive; by clicking or hovering over most widgets, the user can get additional information or follow links to other pages.

Enhancements to the GUI dashboard and its widgets are:

- Multiple dashboard support.
- VDOM and global dashboards.
- Updated resize control for widgets.
- Notifications moved to the top header bar (moved existing dashboard notifications to the header and added additional ones).
- Reorganization of **Add Widget** dialog.
- New **Host Scan Summary** widget.
- New **Vulnerabilities Summary** widget that displays endpoint vulnerability information much like the FortiClient Enterprise Management Server (EMS) summary.
- Multiple bug fixes.



Features that were only visible through old dashboard widgets have been placed elsewhere in the GUI:

- Restore configuration.
- Configuration revisions.
- Firmware management.
- Enabling / disabling VDOMs.
- Changing inspection mode.

- Changing operation mode.
- Shutdown / restart device.
- Changing hostname.
- Changing system time.

The following **widgets are displayed by default**:

- System Information
- Licenses
- FortiCloud
- Security Fabric
- Administrators
- CPU
- Memory
- Sessions
- Bandwidth

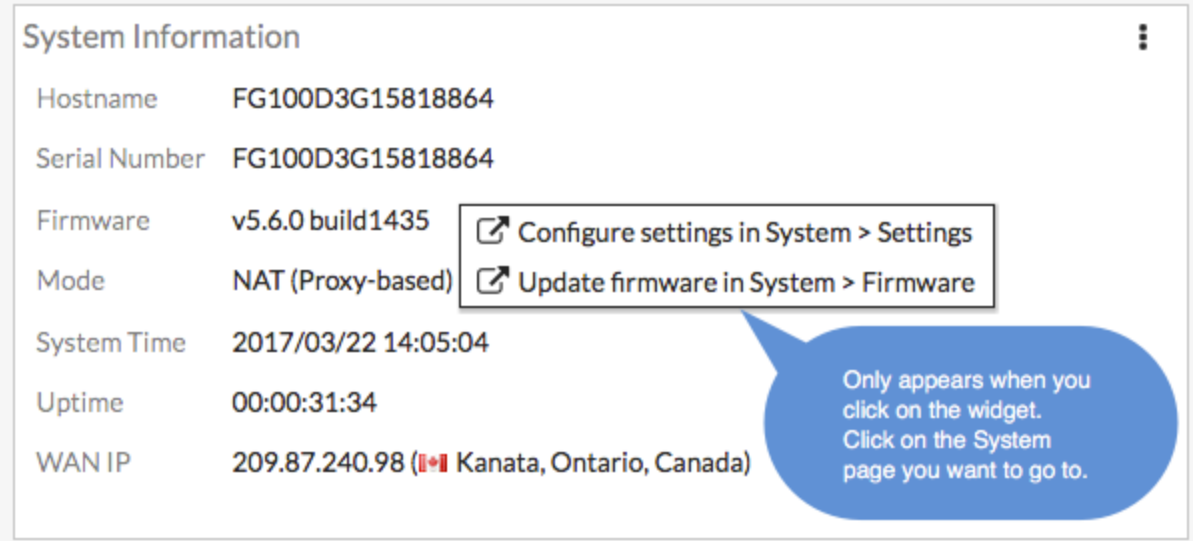
The following **optional** widgets are available:

- Interface Bandwidth
- Disk Usage
- Security Fabric Risk
- Advanced Threat Protection Statistics
- Log Rate
- Session Rate
- Sensor Information
- HA Status
- Host Scan Summary
- Vulnerabilities Summary

The following widgets have been **removed**:

- CLI Console
- Unit Operation
- Alert Message Console

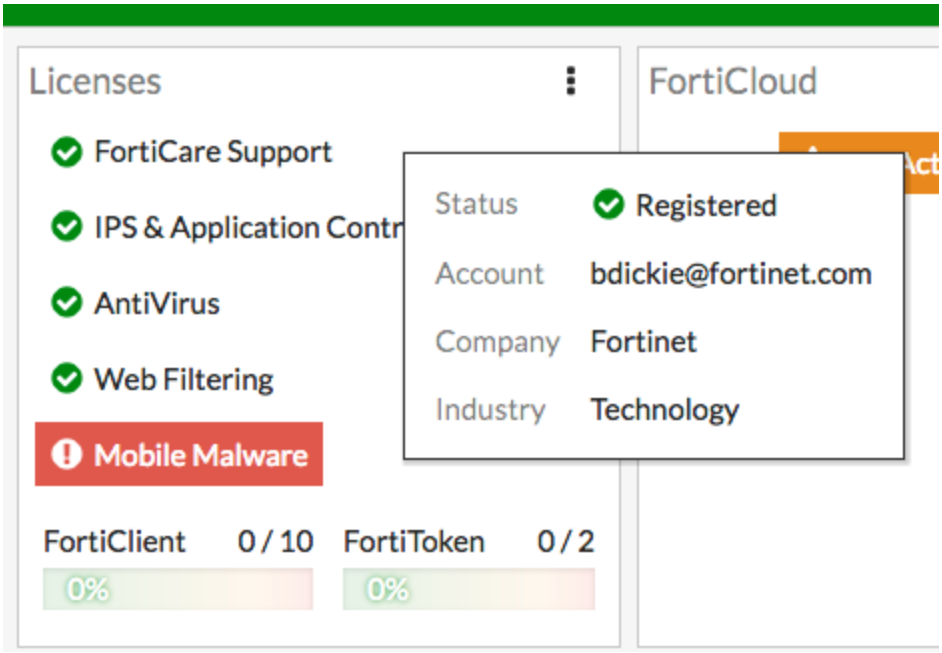
System Information



Licenses

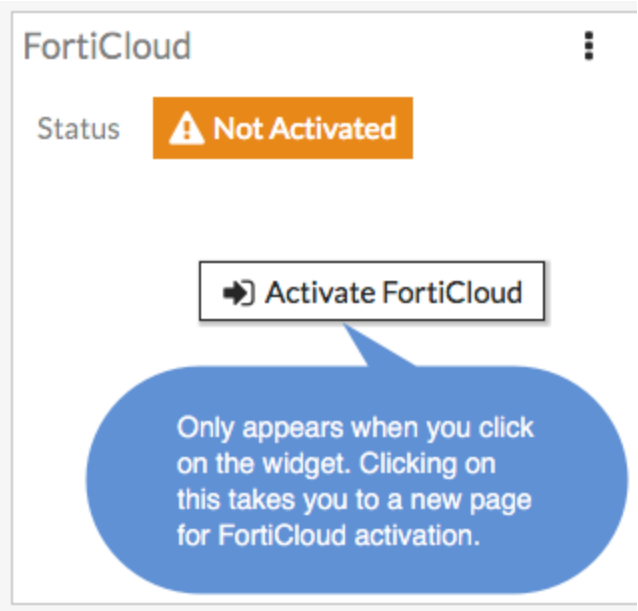
Hovering over the **Licenses** widget will cause status information (and, where applicable, database information) on the licenses to be displayed for **FortiCare Support**, **IPS & Application Control**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, and **FortiClient**. The image below shows **FortiCare Support** information along with the registrant's company name and industry.

Clicking in the **Licenses** widget will provide you with links to other pages, such as **System > FortiGuard** or contract renewal pages.



FortiCloud

This widget displays FortiCloud status and provides a link to activate FortiCloud.

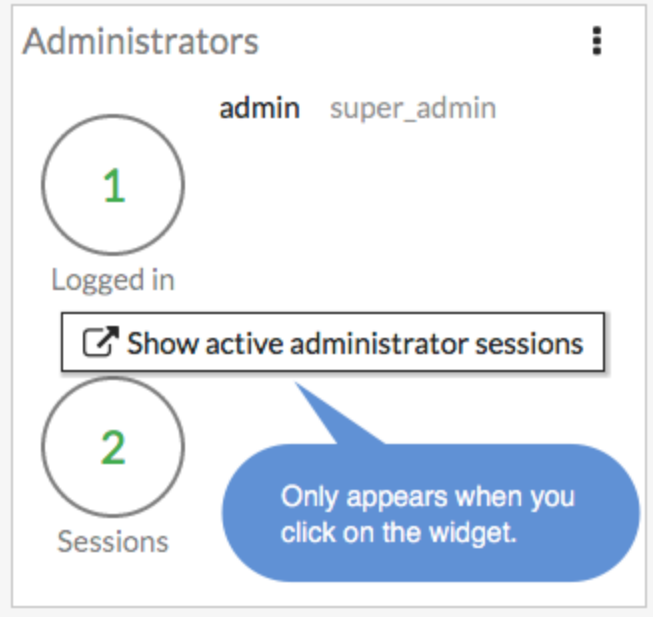


Security Fabric

The **Security Fabric** widget is documented in the Security Fabric section of the **What's New** document.

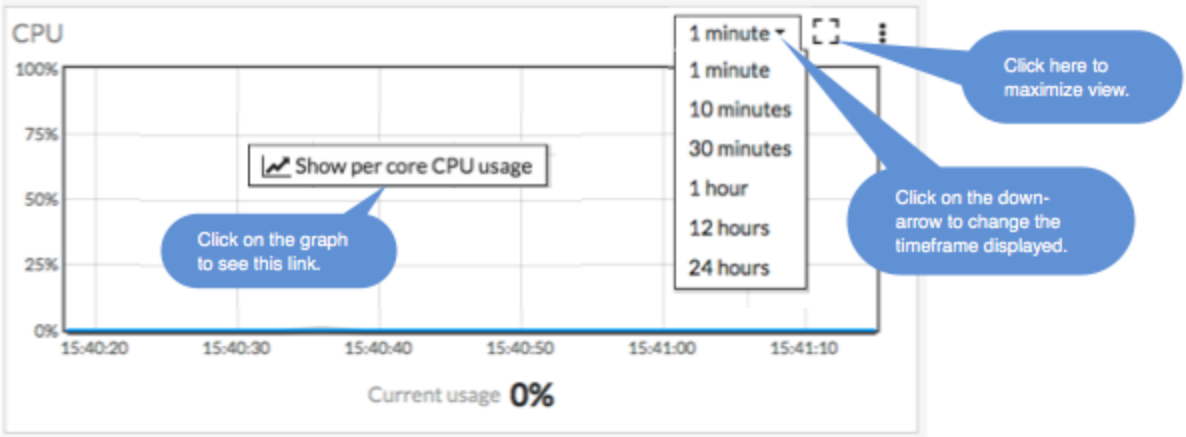
Administrators

This widget allows you to view which administrators are logged in and how many sessions are active. The link directs you to a page displaying active administrator sessions.



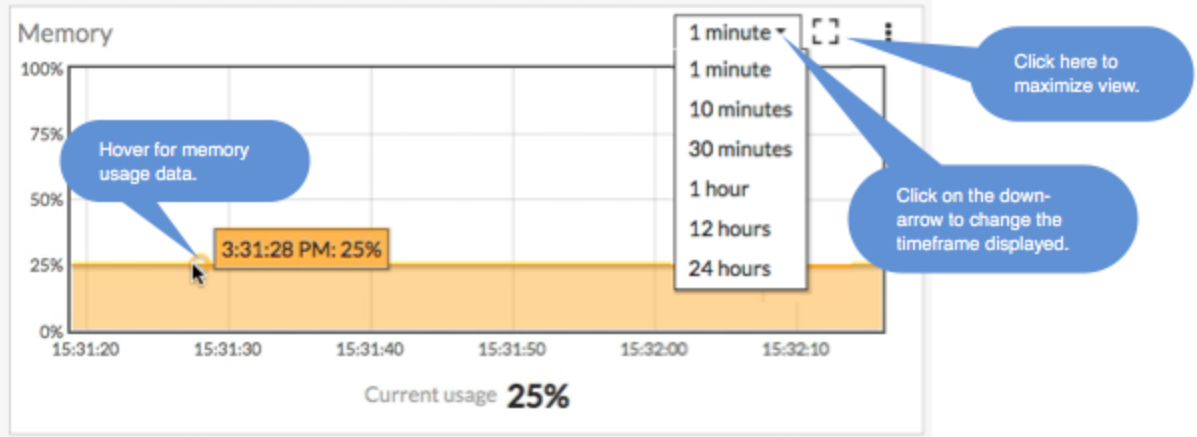
CPU

The real-time CPU usage is displayed for different time frames.

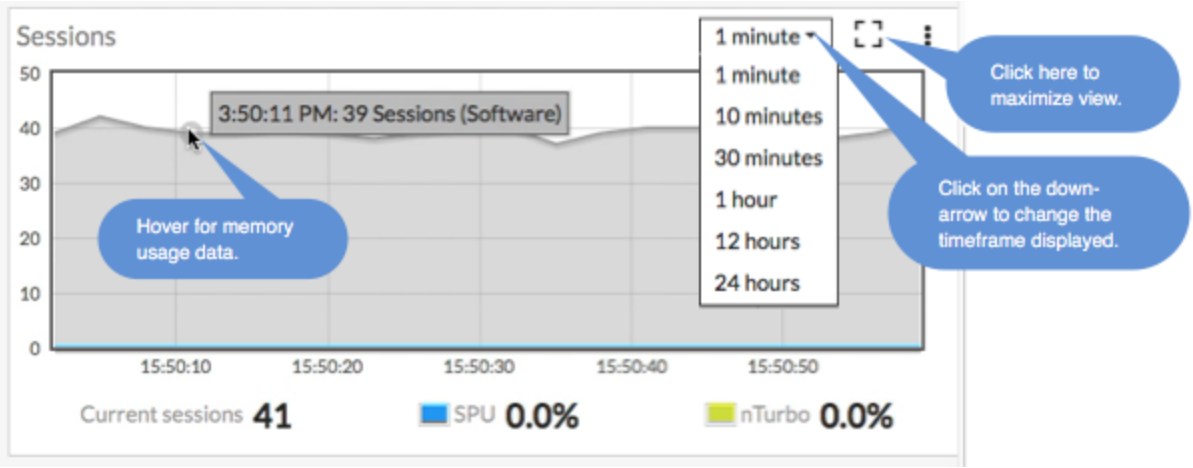


Memory

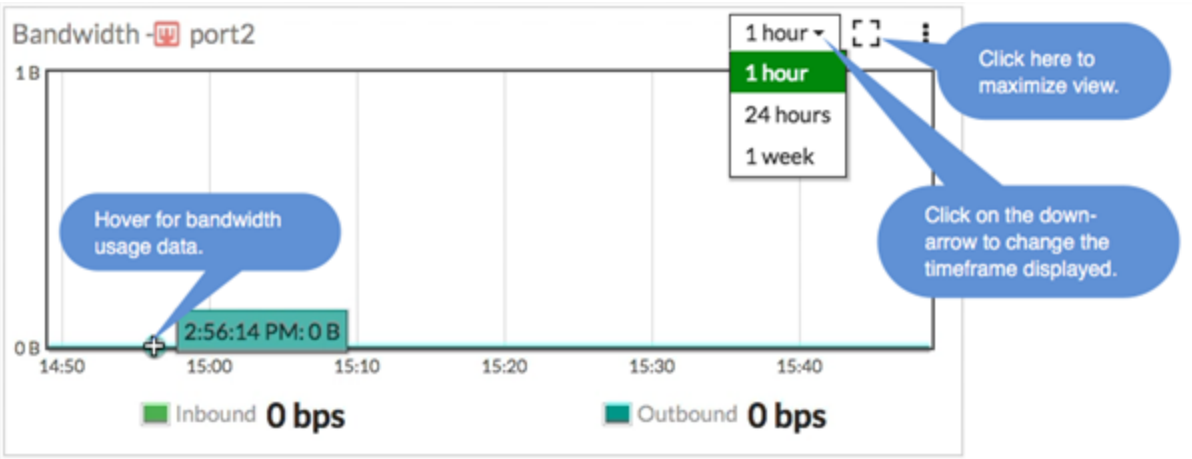
Real-time memory usage is displayed for different time frames. Hovering over any point on the graph displays percentage of memory used along with a timestamp.



Sessions



Bandwidth



FortiExplorer for iOS

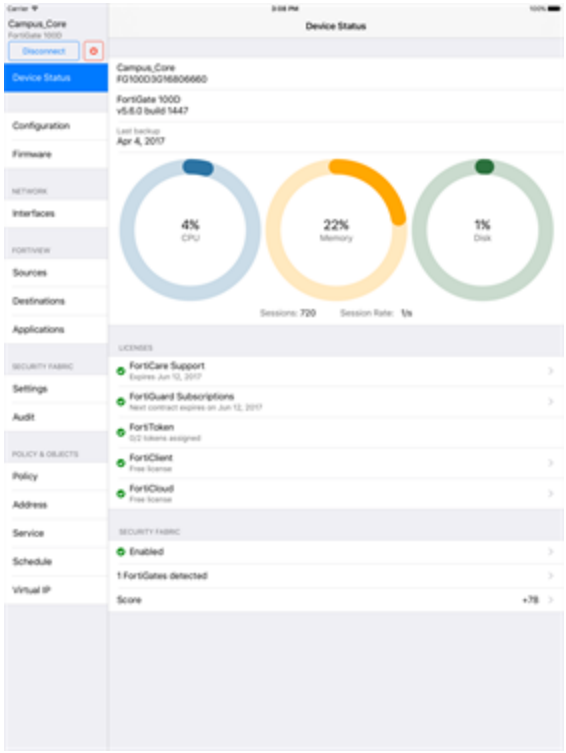
A new iOS FortiExplorer app is available as of April 8, 2017.

FortExplorer for iOS is compatible with iPhone, iPad, and iPod Touch and supports configuration via REST API and display of FortiView and other security fabric components.

You can use FortiExplorer for iOS to perform most FortiOS configuration management tasks.

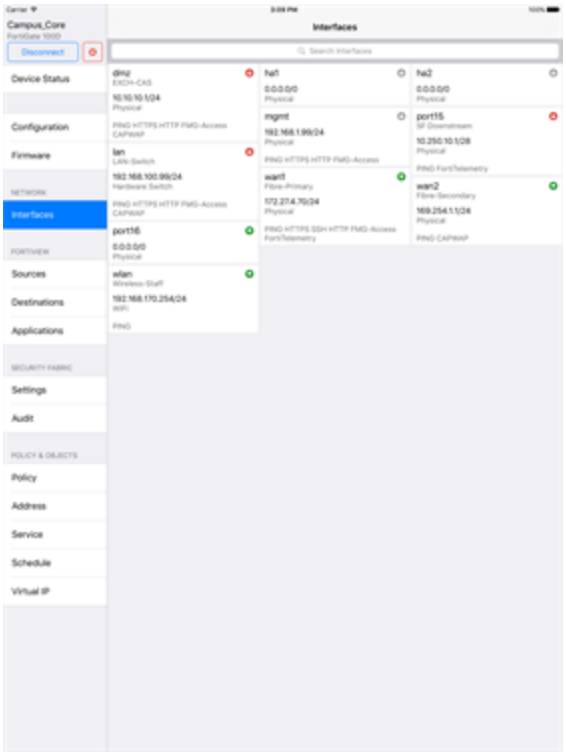
Advanced features will be available with the purchase of an add-on through the App Store. These paid features include the adding more than two devices and downloading firmware images from FortiCare.

The images below offer a preview of a few of the new FortiExplorer iOS app's screens.

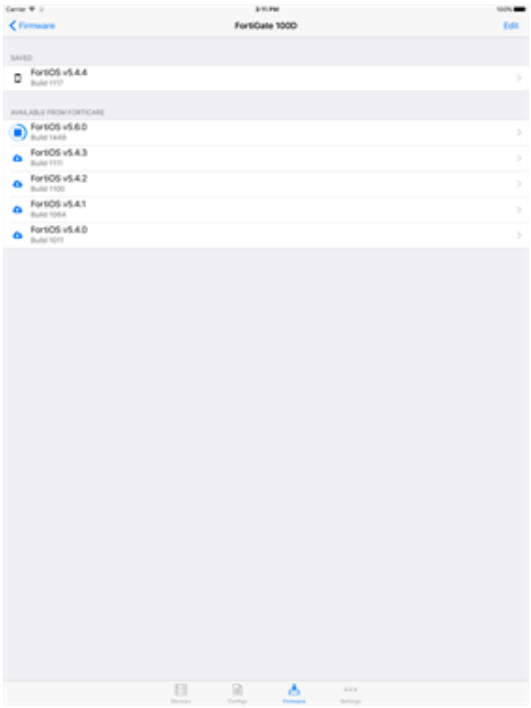


FortiExplorer iOS, v 1.0 - Device Status

FortiExplorer iOS, v. 1.0 - Sources



FortiExplorer iOS, v.1.0 - Device Interfaces



FortiExplorer iOS, v.1.0 - Firmware

Transparent web proxy (386474)

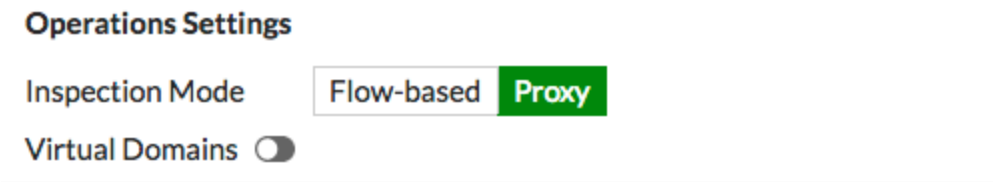
In addition to the Explicit Web Proxy, FortiOS now supports a Transparent web proxy. While it does not have as many features as Explicit Web Proxy, the transparent proxy has the advantage that nothing needs to be done on the user's system to forward supported web traffic over to the proxy. There is no need to reconfigure the browser or publish a PAC file. Everything is transparent to the end user, hence the name. This makes it easier to incorporate new users into a proxy deployment.

You can use the transparent proxy to apply web authentication to HTTP traffic accepted by a firewall policy. In previous versions of FortiOS, web authentication required using the explicit proxy.

Normal FortiOS authentication is IP address based. Users are authenticated according to their IP address and access is allowed or denied based on this IP address. On networks where authentication based on IP address will not work you can use the Transparent Web proxy to apply web authentication that is based on the user's browser and not on their IP address. This authentication method allows you to identify individual users even if multiple users on your network are connecting to the FortiGate from the same IP address.

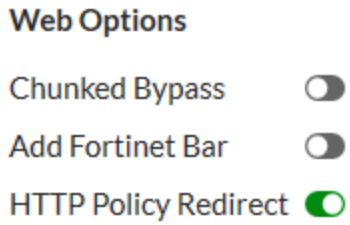
Using the Transparent proxy

To implement the Transparent proxy, go to **System > Settings** and scroll down to **Operations Settings** and set the inspection mode to **Proxy**.



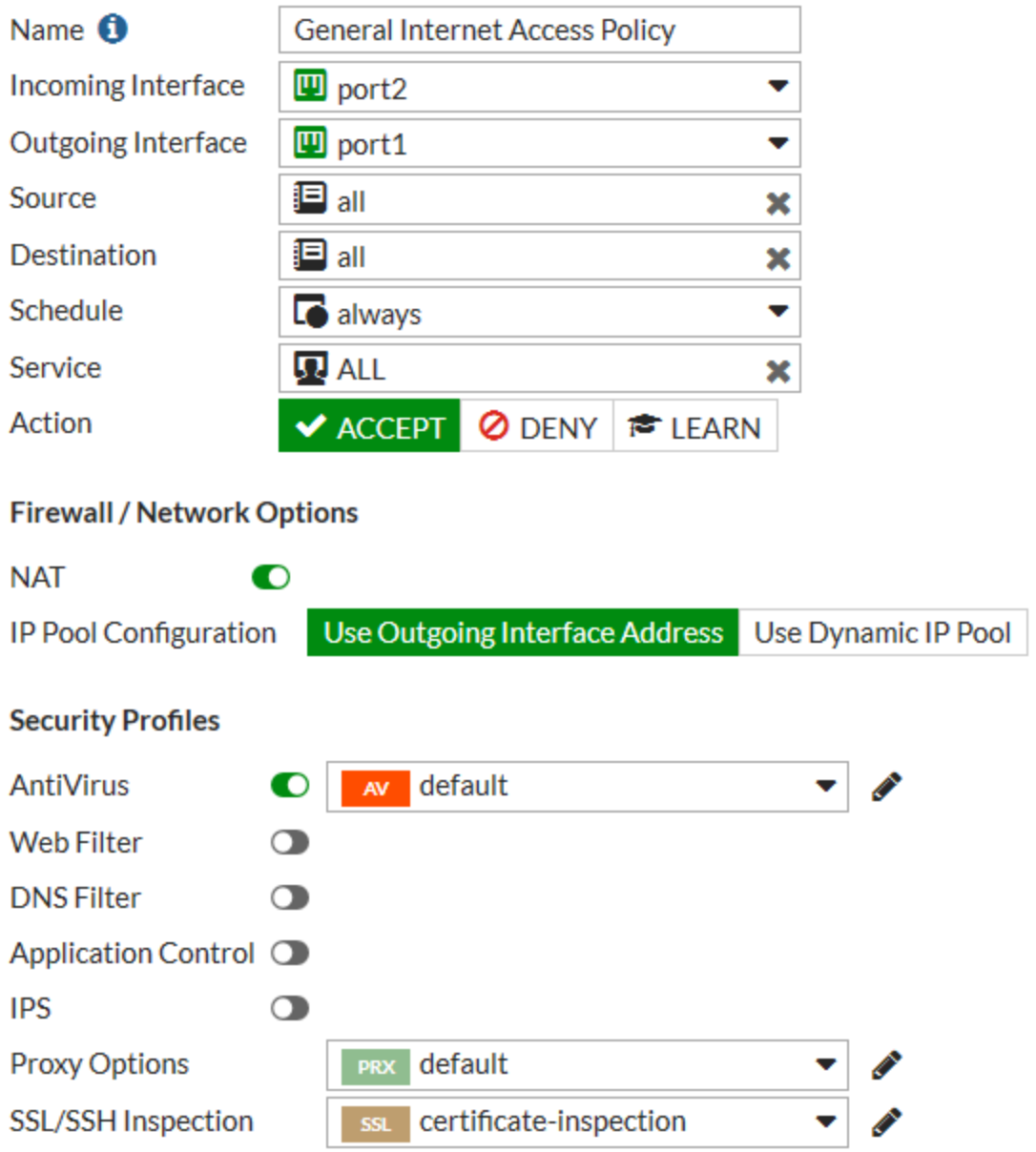
Then go to **System > Feature Select** and enable **Explicit Proxy**.

Then go to **Security Profiles > Proxy Options**, edit a proxy options profile and under **Web Options** enable **HTTP Policy Redirect**.



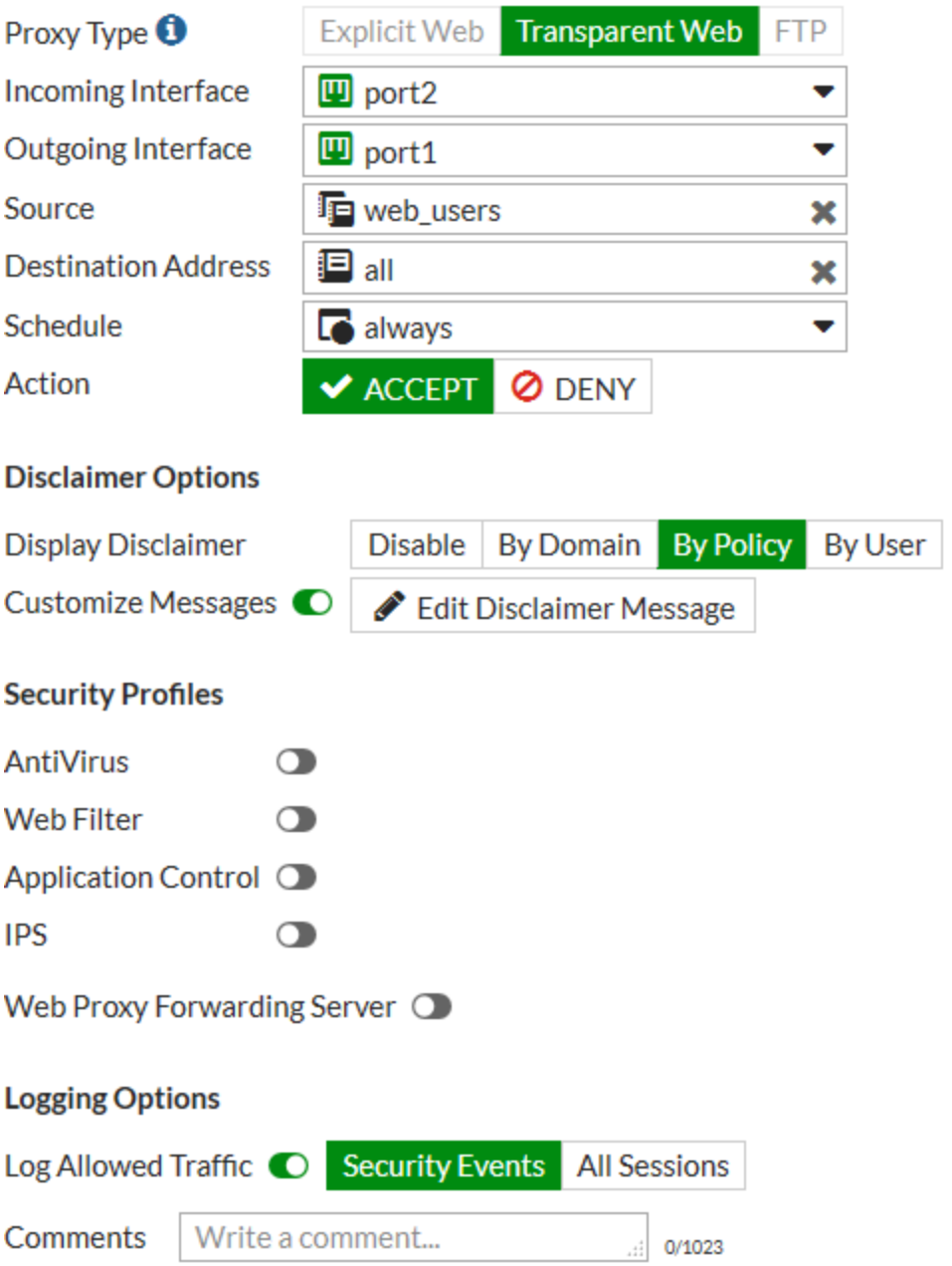
Then go to **Policy & Objects > IPv4 Policy** and create or edit a policy that accepts traffic that you want to apply web authentication to. This can be a general policy that accepts many different types of traffic as long as it also accepts the web traffic that you want to apply web authentication to.

Select a **Security Profile** and select the **Proxy Options** profile that you enabled **HTTP Policy Redirect** for.



Then go to **Policy & Objects > Proxy Policy** create a Transparent Proxy policy to accept the traffic that you want to apply web authentication to. Set the **Proxy Type** to **Transparent Web**. The incoming interface, outgoing interface, destination address, and schedule should either match or be a subset of the same options defined in the IPv4 policy. Addresses added to the Source must match or be a subset of the source addresses added to the IPv4 policy. You can also add the users to be authenticated by the transparent policy to the source field.

Select other transparent policy options as required.



More about the transparent proxy

The following changes are incorporated into Transparent proxy, some of which affect Explicit Web Proxy as well.

Flat policies

The split policy feature has been removed. This will make the explicit policy more like the firewall policy.

Authentication

The new authentication design is intended to separate authentication from authorization. Authentication has been moved into a new table in the FortiOS. This leaves the authorization as the domain of the explicit proxy policy.

Previously, if authentication was to be used:

1. The policy would be classified as an identity based policy
2. The policy would be split to add the authentication parameters
3. The authentication method would be selected
4. The user/group would be configured

Now:

The user/group is configured in the proxy policy

1. A new authentication rule is added
2. This option refers to the authentication scheme
3. The authentication scheme has the details of the authentication method

The new authentication work flow for Transparent Proxy:

Toggle the transparent-http-policy match:

```
config firewall profile-protocol-options
   edit <profile ID>
      config http
         set http-policy <enable|disable>
```

If disabled, everything works like before. If enabled, the authentication is triggered differently.

- http-policy work flow:
- For transparent traffic, if there is a regular firewall policy match, when the Layer 7 check option is enabled, traffic will be redirected to WAD for further processing.
- For redirected traffic, layer 7 policy (HTTP policy) will be used to determine how to do security checks.
- If the last matching factor is down to user ID, then it will trigger a new module to handle the L7 policy user authentication.
- Then propagate learned user information back to the system so that it can be used to match traffic for L4 policy.

New Proxy Type

There is a new subcategory of proxy in the proxy policy called ***Transparent Web***. The old ***Web Proxy*** is now referred to as ***Explicit Web Proxy.***

- This is set in the firewall policy
- It is available when the HTTP policy is enabled in the profile-protocol options for the firewall policy
- This proxy type supports OSI layer 7 address matching.
- This proxy type should include a source address as a parameter
- Limitations:
  - It can be used for HTTPS traffic, if deep scanning is not used
  - It only supports SNI address matching, i.e. domain names

- It does not support header types of address matching
- It only supports SSO authentication methods, no active authentication methods.

IP pools support

Proxies are now supported on outgoing IP pools.

SOCKSv5

SOCKSv5 authentication is now supported for explicit proxies.

To configure:

```
config authentication rule
   edit <name of rule>
      set protocol socks
      end
```

Forwarding

Proxies support URL redirect/forwarding. This allows a non-proxy forwarding server to be assigned a rule that will redirect web traffic from one URL to another, such as redirecting traffic destined for youtube.com to restrict.youtube.com.

- A new option called "Redirect URL" has been added to the policy
- Traffic forwarding by VIP is supported

Support for explicit proxy address objects & groups into IPv4 firewall policies

This would allow the selection of web filter policy, SSL inspection policy, and proxy policy based on source IP + destination (address|explicit proxy object|category|group of any of those). This enables things like “do full SSL interception on www.google.com, but not the rest of the Search Engines category”.

Support application service in the proxy based on HTTP requests.

The application service can be configured using the following CLI commands:

```
config firewall service custom
   edit <name of service>
   set explicit-proxy enable
   set app-service-type <disable|app-id|app-category>
   set app-category <application category ID, integer>
   set application <application ID, integer>
   end
```

CLI

Changes:

Previous	New
config firewall explicit-proxy-policy	config firewall proxy-policy
config firewall explicit-proxy-address	config firewall proxy-address
config firewall explicit-proxy-addrgrp	config firewall proxy-addrgrp
config firewall explicit-proxy-policy edit <policy ID> set proxy web end	config firewall proxy-policy edit <policy ID> set proxy explicit-web end

Removals:

- "split-policy" from firewall explicit-proxy-policy.

  The previous method to set up a split policy was:

```
config firewall explicit-proxy-policy
   edit 1
      set proxy web
      set identity-based enable
      config identity-based-policy
         edit 1
            set schedule "always"
            set utm-status enable
            set users "guest"
            set profile-protocol-options "default"
            next
         end
      next
   end
```

- "auth relative" from firewall explicit-proxy-policy

  The following attributes have been removed from firewall explicit-proxy-policy:

  - identity-based
  - ip-based
  - active-auth-method
  - sso-auth-method
  - require-tfa

Moves:

users and groups from

```
firewall explicit-proxy-policy identity-based-policy
```

to

```
config firewall proxy-policy
   edit 1
   set groups <Group name>
   set users <User name>
   end
```

Additions:

authentication scheme

```
config authentication scheme
   edit <name>
      set method [ntlm|basic|digest|form|negotiate|fsso|rsso|none]
```

- `ntlm` - NTLM authentication.
- `basic` - Basic HTTP authentication.
- `digest` - Digest HTTP authentication.
- `form` - Form-based HTTP authentication.
- `negotiate` - Negotiate authentication.
- `fsso` - FSSO authentication.
- `rsso` - RADIUS Single Sign-On authentication.
- `none` - No authentication.

authentication setting

```
config authentication setting
   set active-auth-scheme <string>
   set sso-auth-scheme <string>
   set captive-portal <string>
   set captive-portal-port <integer value from 1 to 65535>
```

- `active-auth-scheme` - Active authentication method.
- `sso-auth-scheme` - SSO authentication method.
- `captive-portal` - Captive portal host name.
- `captive-portal-port` - Captive portal port number.

authentication rule

```
config authentication rule
   edit <name of rule>
      set status [enable|disable]
      set protocol [http|ftp|socks]
      set srcaddr <name of address object>
      set srcaddr6 <name of address object>
      set ip-based [enable|disable]
      set active-auth-method <string>
      set sso-auth-method <string>
      set web-auth-cookie [enable|disable]
      set transaction-based [enable|disable]
      set comments
```

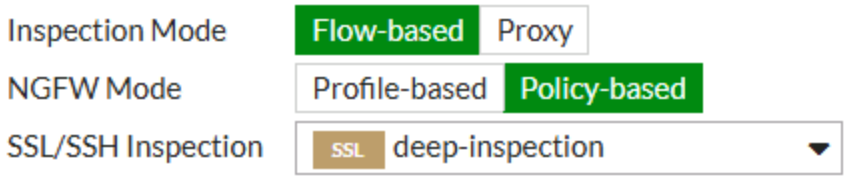
- `status` - Enable/disable auth rule status.
- `protocol` - set protocols to be matched
- `srcaddr /srcaddr6` - Source address name. [srcaddr or srcaddr6(web proxy only) must be set].
- `ip-based` - Enable/disable IP-based authentication.
- `active-auth-method` - Active authentication method.
- `sso-auth-method` - SSO authentication method (require `ip-based` enabled)
- `web-auth-cookie` - Enable/disable Web authentication cookie.
- `transaction-based` - Enable/disable transaction based authentication.
- `comments` - Comment.

NGFW Policy Mode (371602)

You can operate your FortiGate or individual VDOMs in **Next Generation Firewall (NGFW) Policy Mode**.

You can enable NGFW policy mode by going to **System > Settings**, setting the **Inspection mode** to **Flow-based** and setting the NGFW mode to **Policy-based**. When selecting **NGFW policy-based** mode you also select the SSL/SSH Inspection mode that is applied to all policies

Flow-based inspection with profile-based **NGFW mode** is the default in FortiOS 5.6.

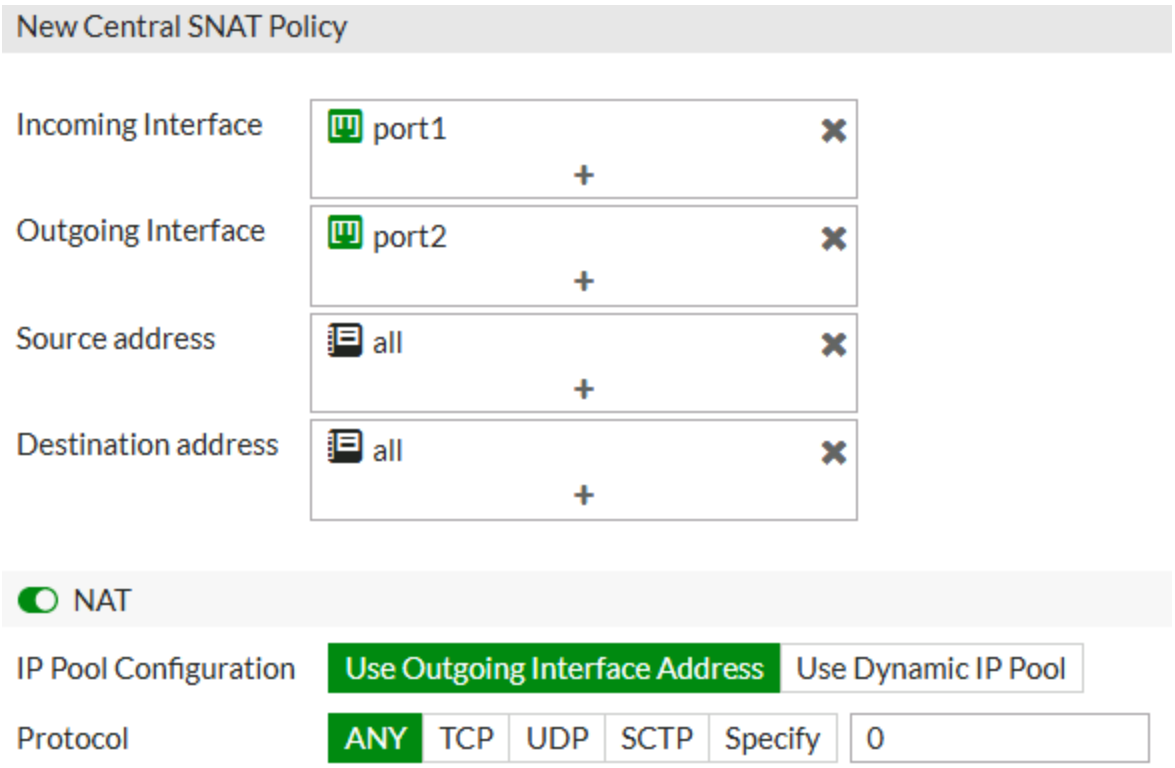


Or use the following CLI command:

```
config system settings
   set inspection-mode flow
   set policy-mode {standard | ngfw}
end
```

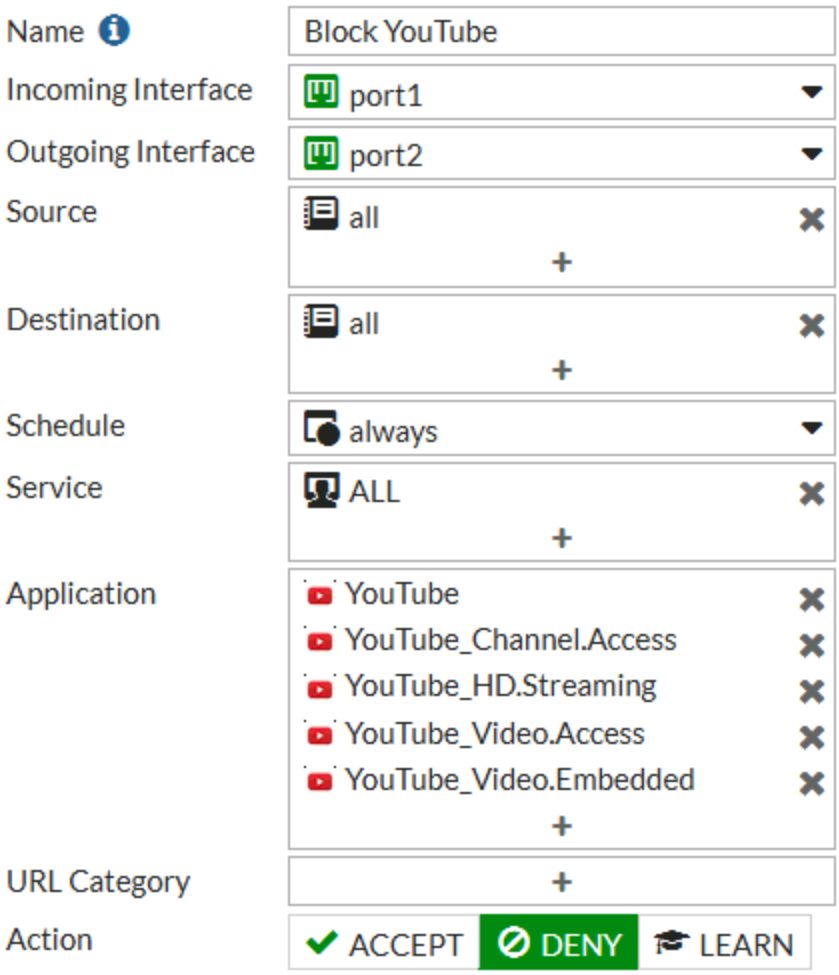
NGFW policy mode and NAT

If your FortiGate is operating in NAT mode, rather than enabling source NAT in individual NGFW policies you go to **Policy & Objects > Central SNAT** and add source NAT policies that apply to all matching traffic. In many cases you may only need one SNAT policy for each interface pair. For example, if you allow users on the internal network (connected to port1) to browse the Internet (connected to port2) you can add a port1 to port2 Central SNAT policy similar to the following:



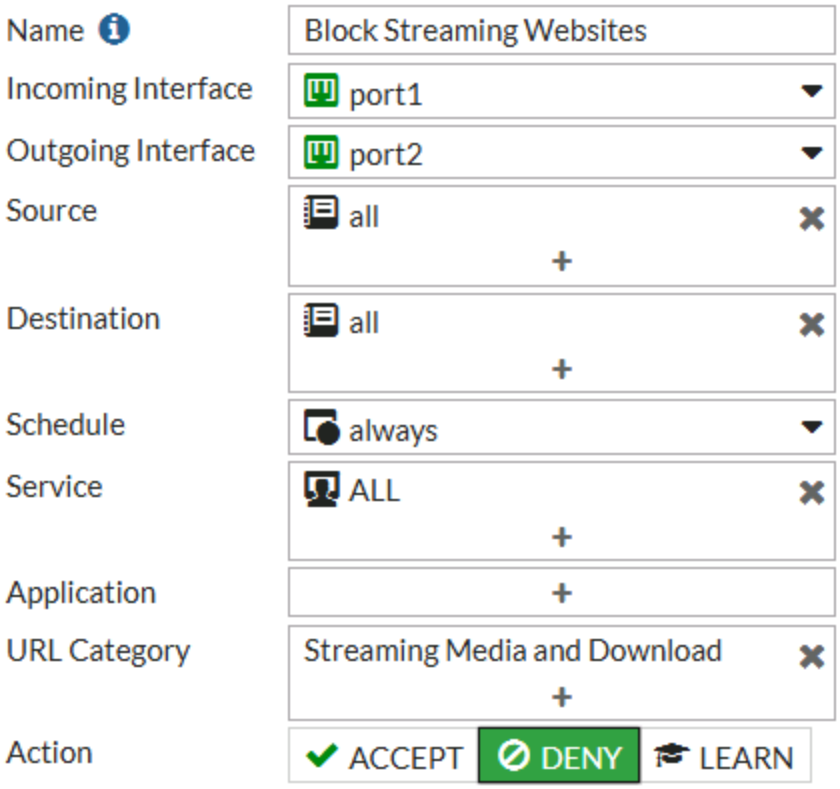
Application control in NGFW policy mode

You configure **Application Control** simply by adding individual applications to security policies. You can set the action to accept or deny to allow or block the applications.



Web Filtering in NGFW mode

You configure **Web Filtering** by adding URL categories to security policies. You can set the action to accept or deny to allow or block the applications.

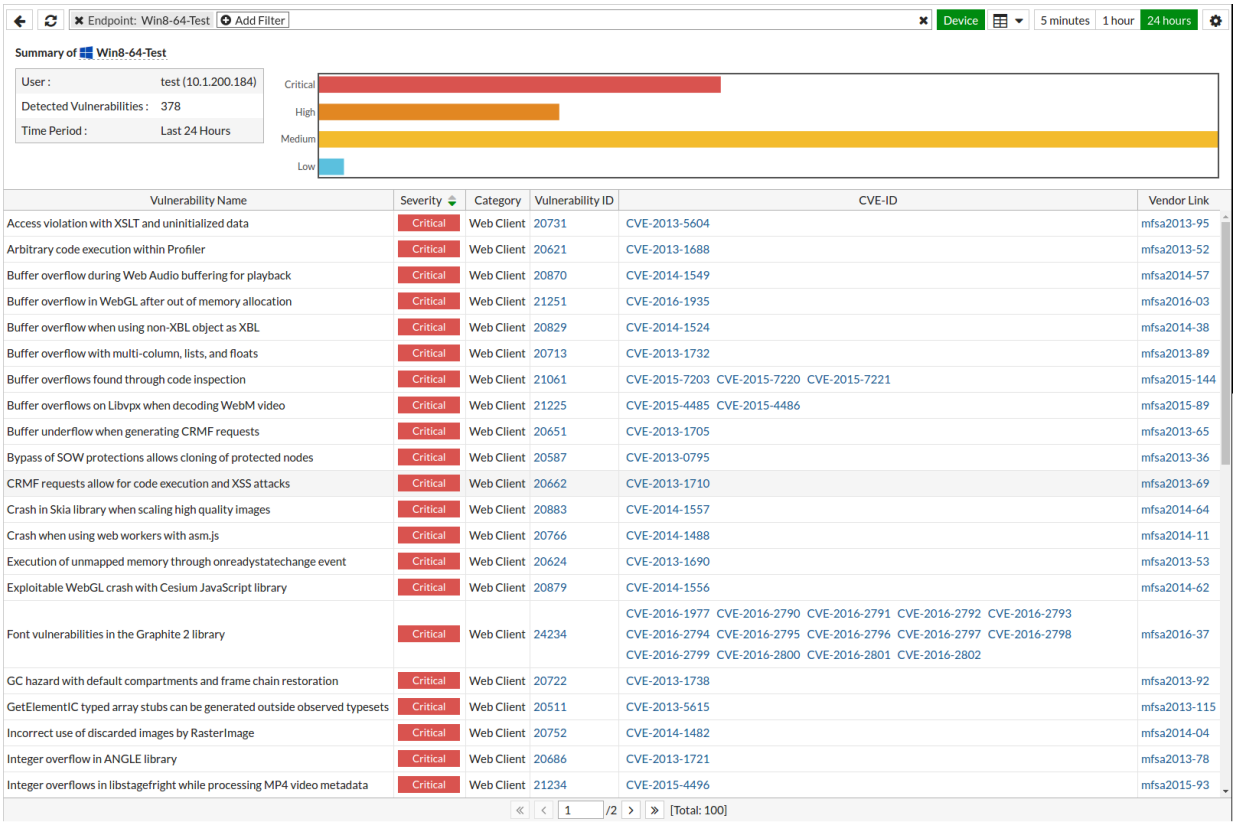


Other NGFW policy mode options

You can also combine both application control and web filtering in the same NGFW policy mode policy. Also if the policy accepts applications or URL categories you can also apply Antivirus, DNS Filtering, and IPS profiles in NGFW mode policies as well a logging and policy learning mode.

New FortiView Endpoint Vulnerability Scanner chart (378647)

FortiOS 5.6.0 adds a new chart to illustrate Endpoint Control events: **Endpoint Vulnerability**.
This is a list/bubble chart, that tracks vulnerability events detected by the FortiClients running on all devices registered with the FortiGate. FortiView displays information about the vulnerability and the device on which it was detected.



Notes about the Endpoint Vulnerability Chart:

- You can sort the list by **Device** or **Vulnerability**.
- You can drill down into any device to see the Vulnerabilities detected. From there, you can drill down to see the exact Vulnerability Scan events that triggered the detection.
- Select any Vulnerability Scan event to see the associated Log data.

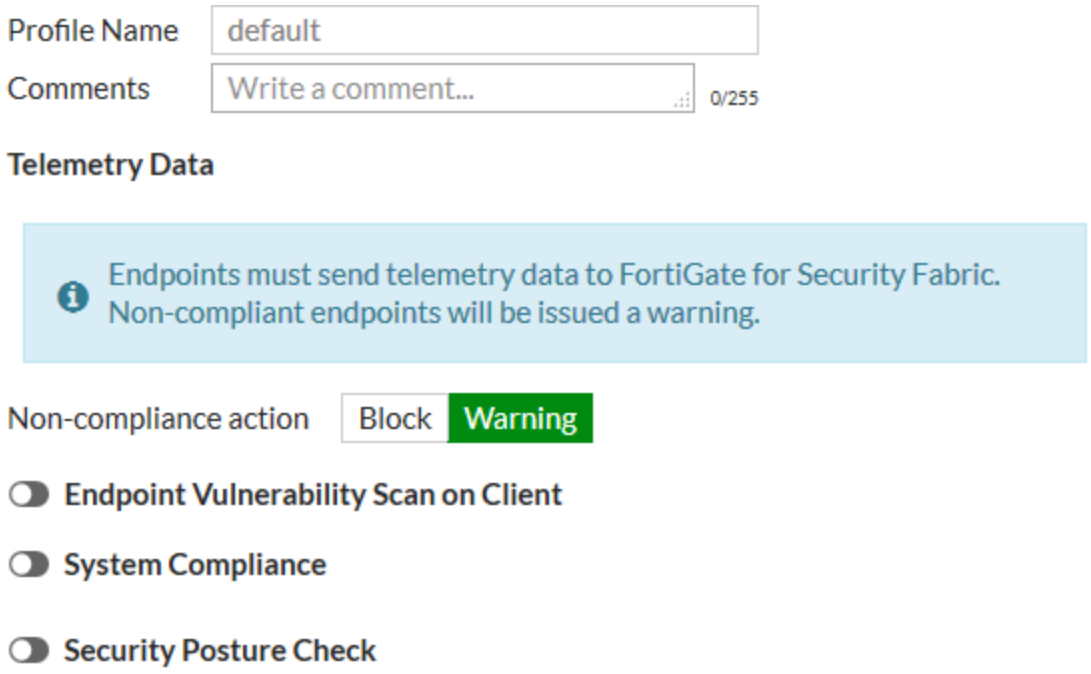
FortiClient Profile changes (386267, 375049)

FortiClient profiles have been changed in FortiOS 5.6 to include new protection features and to change organization of the GUI options. FortiClient profiles also use the FortiGate to warn or quarantine endpoints that are not compliant with a FortiClient profile.

A bug that prevented the Dialog and Device Inventory pages from loading when there is a large number of devices (for example, 10,000) has been fixed.

Default FortClient profile

FortiClient profiles allow you to perform vulnerability scans on endpoints and make sure endpoints are running compliant versions of FortiClient. Also, security posture features cause FortiClient to apply realtime protection, AntiVirus, web filtering, and application control on endpoints.



The default FortiClient profile also allows you to set a general **Non-compliance action** for endpoints that don't have FortiClient installed on them. The non-compliance action can be block or warning and is applied by the FortiGate. Blocked endpoints are quarantined by the FortiGate.

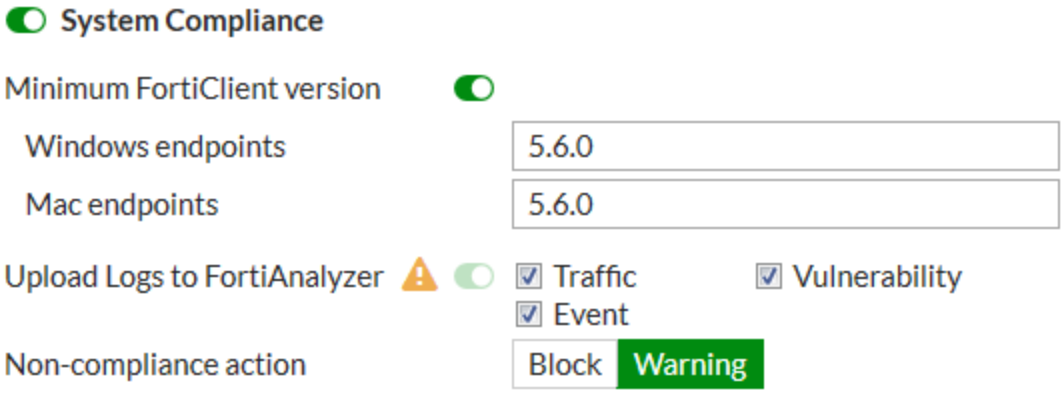
Endpoint vulnerability scanning

Similar to FortiOS 5.4 you can set the FortiClient Profile to run the FortiClient vulnerability scanner on endpoints and you can set the Vulnerability quarantine level to quarantine endpoints that don't comply.

The vulnerability scan **Non-compliance action** can block or warn endpoints if the vulnerability scan shows they do not meet the vulnerability quarantine level.

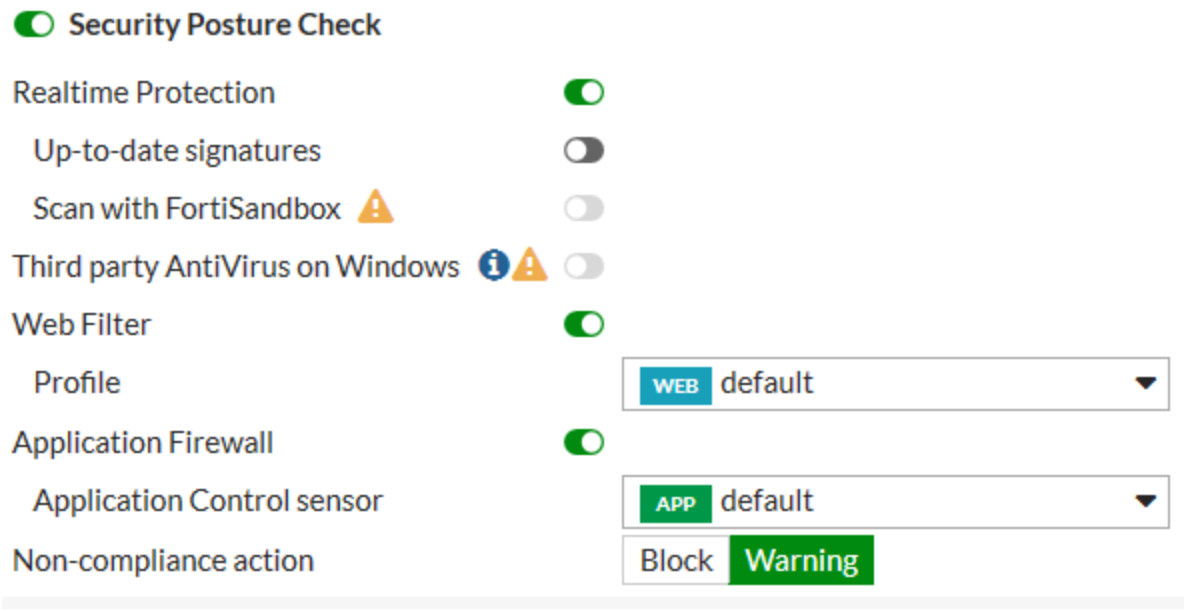
System compliance

FortiOS 5.6 system compliance settings are similar to those in 5.4 with the addition of a non-compliance action. System compliance checking is performed by FortiClient but the non-compliance action is applied by the FortiGate.



Security posture checking

Security posture checking collects realtime protection, antivirus protection, web filtering and application firewall features under the **Security Posture Check** heading.


Security Posture Check
Realtime Protection
Up-to-date signatures
Scan with FortiSandbox
Third party AntiVirus on Windows
Web Filter
Profile
WEB default
Application Firewall
Application Control sensor
APP default
Non-compliance action
Block
Warning

Application Control is a free service

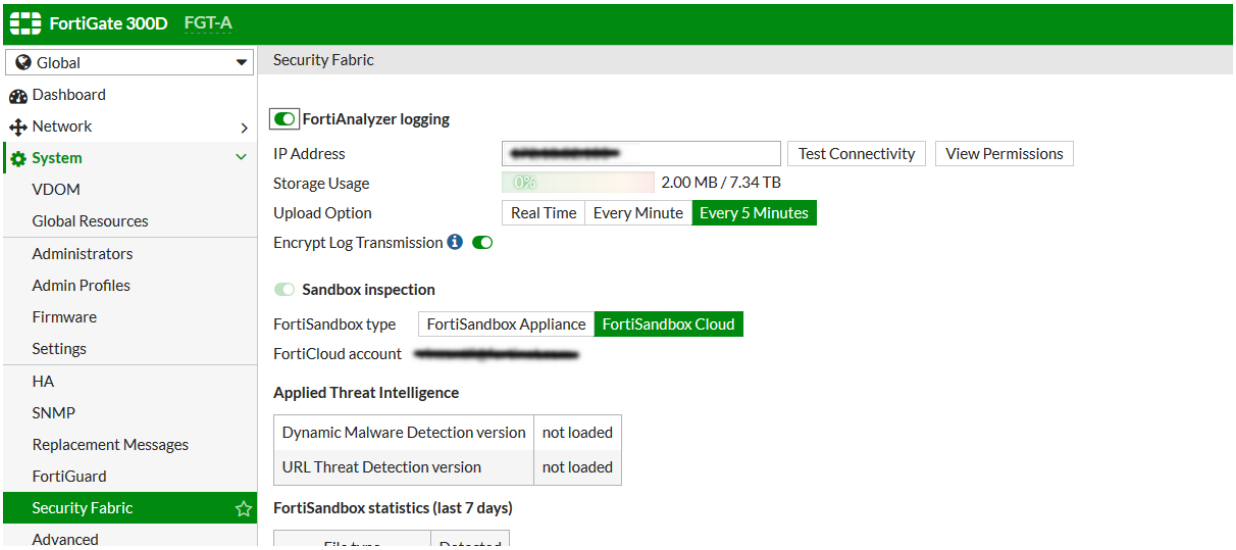
Application Control is now a free FortiGuard service and the database for Application Control signatures is separate from the IPS database. However, Botnet Application signatures are still part of the IPS signature database since these are more closely related with security issues and less about application detection.

IPS / Application Control logging performance

There is a major boost to Application Control and IPS when logging is enabled. With the latest changes, the performance difference with or without logging enabled is negligible.

Real time logging to FortiAnalyzer and FortiCloud

FortiOS 5.6.0 adds new real-time logging options for FortiAnalyzer in **System > Security Fabric** and for FortiCloud in **Log & Report > Log Settings**. The default option is still every 5 minutes, but this will allow near real-time uploading and consistent high-speed compression and analysis.



For FortiAnalyzer, the CLI syntax to enable real-time is:

```
config log fortianalyzer setting
   set upload-option [realtime/1-minute/5-minute]
```

For FortiCloud:

```
config log fortiguard setting
   set upload-option [realtime/1-minute/5-minute]
```

Reliable Logging updated for real-time functionality (378937)

Previously, reliable logging was a feature for buffering and collecting logs for upload, to guarantee that no logs would be dropped before being passed to logging solutions. Reliable logging has been updated for 5.6.0 and is now enabled by default, so that real-time logs do not outpace upload speed.

It can be configured in the CLI with:

```
config log fortianalyzer setting
   set reliable [enable/disable]
```

FortiGate Logs can be sent to syslog servers in Common Event Format (CEF) (300128)

You can configure FortiOS to send log messages to remote syslog servers in CEF format. CEF is an open log management standard that provides interoperability of security-related information between different network devices and applications. CEF data can be collected and aggregated for analysis by enterprise management or Security Information and Event Management (SIEM) systems such as FortiSIEM.

FortiOS supports logging to up to four remote syslog servers. Each server can now be configured separately to send log messages in CEF or CSV format. Previously only CSV format was supported.

Use the following command to configure syslog3 to use CEF format:

```
config log syslog3 setting
   set format cef
end
```

All other syslog settings can be configured as required independently of the log message format including the server address and transport (UDP or TCP). You can also configure filtering for both CEF and CSV formatted log messages.

Controlled failover between wireless controllers

1+1 Wireless Controller HA

Instances of failover between FortiAP units was too long and lead to extended periods of time where WiFi users were without network connection. Because WiFi is considered a primary network connection in today's verticals (including enterprise, retail, education, warehousing, healthcare, government, and more), it is necessary for successful failover to occur as fast as possible.

Primary and secondary ACs

You can now define the role of the primary and secondary controllers on the FortiAP unit, allowing the unit to decide the order in which the FortiAP selects the FortiGate. This process was previously decided on load-based detection, but can now be defined by each unit's pre-determined priority. In addition, heartbeat intervals have been lowered to further improve FortiAP awareness and successful failover.

The **Managed FortiAP** in **Branch office** is managed by the primary AC, **FortiGate 4**, in the **HQ** location. If the primary unit fails, the FortiAP will then be managed by the secondary AC, **FortiGate 5**.

1+1 redundancy

1+1 HA is a form of resilience whereby a component has a backup component to take its place in the event of component failure, and successfully manage FortiAP without long failover periods.

CLI syntax

```
config wireless-controller inter-controller
   set inter-controller-mode {disable | l2-roaming | 1+1} Default is disable.
   set inter-controller-key <password>
   set inter-controller-pri {primary | secondary} Default is primary.
   set fast-failover-max [3-64] Default is 10.
   set fast-failover-wait [10-86400] Default is 10.
   config inter-controller-peer
      edit <name>
         set peer-ip <ip-address>
         set peer-port [1024-49150] Default is 5246.
         set peer-priority {primary | secondary} Default is primary.
      next
   end
end
```

Multiple PSK for WPA Personal (393320)

New CLI commands have been added, under `config wireless-controller vap`, to configure multiple WiFi Protected Access Pre-Shared Keys (WPA-PSKs), as PSK is more secure without all devices having to share the same PSK.

Note that `mpsk-concurrent-clients` and the `mpsk-key` configuration method are only available when `mpsk` is set to `enable`.

CLI syntax

```
config wireless-controller vap
   edit <example>
      set mpsk {enable|disable}
      set mpsk-concurrent-clients [0-65535] Default is 0.
      config mpsk-key
         edit <key-name>
            set passphrase <wpa-psk>
            set concurrent-clients [0-65535] Default is empty.
            set comment <comments>
         next
      end
end
```

Use the `mpsk-concurrent-clients` entry to set the maximum number of concurrent connected clients for each `mpsk` entry. Use the `mpsk-key` configuration method to configure multiple `mpsk` entries.

VXLAN support (289354)

Virtual Extensible LAN (VXLAN) is a network virtualization technology used in large cloud computing deployments. It encapsulates OSI layer 2 Ethernet frames within layer 3 IP packets using standard destination port 4789. VXLAN endpoints that terminate VXLAN tunnels can be virtual or physical switch ports, are known as VXLAN tunnel endpoints (VTEPs). For more information about VXLAN, see RFC 7348.

VTEP (VXLAN Tunnel End Point) support (289354)

Native VXLAN is now supported by FortiOS. This feature is configurable from the CLI only:

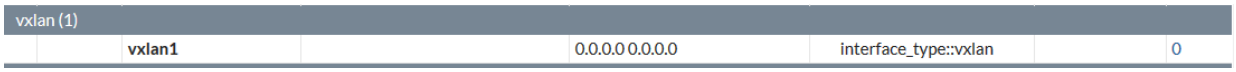
Syntax

```
config system vxlan
   edit <vxlan1> //VXLAN device name (Unique name in system.interface).
      set interface //Local outgoing interface.
      set vni //VXLAN network ID.
      set ip-version //IP version to use for VXLAN device (4 or 6).
      set dstport //VXLAN destination port, default is 4789.
      set ttl //VXLAN TTL.
      set remote-ip //Remote IP address of VXLAN.
   next
end
```

This will create a VXLAN interface:

```
show system interface vxlan1
   config system interface
      edit "vxlan1"
         set vdom "root"
         set type vxlan
         set snmp-index 36
         set macaddr 8a:ee:1d:5d:ae:53
         set interface "port9"
      next
   end
```

From the GUI, go to **Network > Interfaces** to verify the new VXLAN interface:



To diagnose your VXLAN configuration, from the CLI, use the following command:

```
diagnose sys vxlan fdb list vxlan1
```

This command provides information about the VXLAN forwarding data base (fdb) associated to the vxlan1 interface. Below is a sample output:

```
----------mac=00:00:00:00:00:00 state=0x0082 flags=0x00----------
----------remote_ip=2.2.2.2 remote_port=4789----------
----------remote_vni=1 remote_ifindex=19----------
total fdb num: 1
```

VXLAN support for multiple remote IPs (398959)

VXLAN is now supported for multiple remote IPs, these remote IPs can be IPv4 unicast, IPv6 unicast, IPv4 multicast, or IPv6 multicast. This is useful in datacenter scenarios where the FortiGate can be configured with multiple tunnels to computer nodes.

CLI changes

`set ip-version` option can be set to the following:

`ipv4-unicast` //Use IPv4 unicast addressing for VXLAN.

`ipv6-unicast` //Use IPv6 unicast addressing for VXLAN.

`ipv4-multicast` //Use IPv4 multicast addressing for VXLAN.

`ipv6-multicast` //Use IPv6 multicast addressing for VXLAN.

When `ip-version` is set to `ipv4-multicast` or `ipv6-multicast`, `ttl` option is replaced by `multicast-ttl`.

New PPPoE features

PPPoE dynamic gateway support (397628)

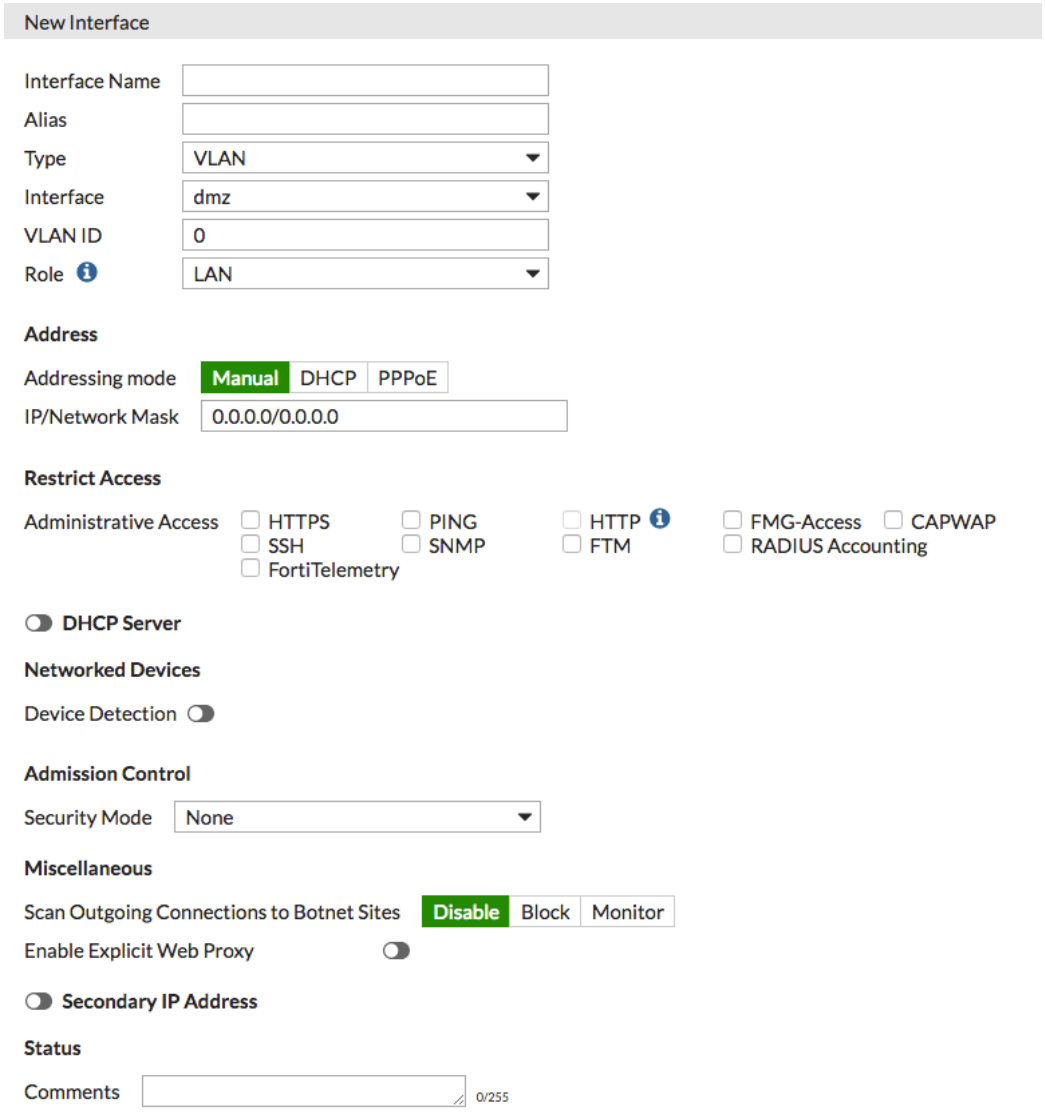
Original design for PPPoE requires to configure a static gateway. Although it works in many scenarios, some customers require to add support for dynamic gateway for internet-service based routes.

No changes to the CLI neither to the GUI.

Support multiple PPPoE connections on a single interface (363958)

Multiple PPPoE connections on a single physical or vlan interface are now supported by the FortiGate. In addition the interface can be on demand PPPoE.

GUI



CLI

```
config system pppoe-interace
   edit <name>
      set dial-on-demand [enable|disable]
      set ipv6 [enable|disable]
      set device <interface>
      set username <string>
      set password <string>
      set auth-type [auto|pap|chap|mschapv1|mschapv2]
      set ipunnumbered <class_ip>
      set pppoe-unnumbered-negotiate [enable|disable]
      set idle-timeout <integer>
      set disc-retry-timeout <integer>
      set padt-retry-timeout <integer>
      set service-name <string>
      set ac-name <string>
```

```
        set lcp-echo-interval <integer>
        set lcp-max-echo-fails <integer>
```

- `dial-on-demand`- Enable/disable the dial on demand.feature
- `ipv6` - Enable/disable the use of IPv6.
- `device` - The name of the physical interface.
- `username` - User name for credentials
- `password` - Password matching the above username
- `auth-type` - The type of PPP authentication to be used.
  - `auto` - Automatic choice of authentication
  - `pap` - PAP authentication
  - `chap` - CHAP authentication
  - `mschapv1` - MS-CHAPv1 authentication
  - `mschapv2` - MS-CHAPv2 authentication
- `ipunnumbered` - PPPoE unnumbered IP.
- `pppoe-unnumbered-negotiate` - Enable/disable PPPoE unnumbered negotiation.
- `idle-timeout` - Idle time in seconds before PPPoE auto disconnects. `0` (zero) for no timeout.
- `disc-retry-timeout` - Timeout value in seconds for PPPoE initial discovery. `0` to `4294967295`. Default = `1`.
- `padt-retry-timeout` - Timeout value in seconds for PPPoE terminatation. `0` to `4294967295`. Default = `1`.
- `service-name` - PPPoE service name.)
- `ac-name` - PPPoE AC name.
- `lcp-echo-interval` - Interval in seconds allowed for PPPoE LCP echo. `0` to `4294967295`. Default = `5`.
- `lcp-max-echo-fails` - Maximum number of missed LCP echo messages before disconnect. `0` to `4294967295`. Default = 3.

Adding Internet services to firewall policies (389951)

In 5.4, support was added for Internet Service objects which could be used with ***FortiView***, ***Logging***, ***Routing*** and ***WAN Load Balancing***. Now they can be added to firewall policies as well.

There is an either or relationship between Internet Service objects and destination address and service combinations in firewall policies. This means that a destination address and service can be specified in the policy OR an Internet service, not both.

CLI

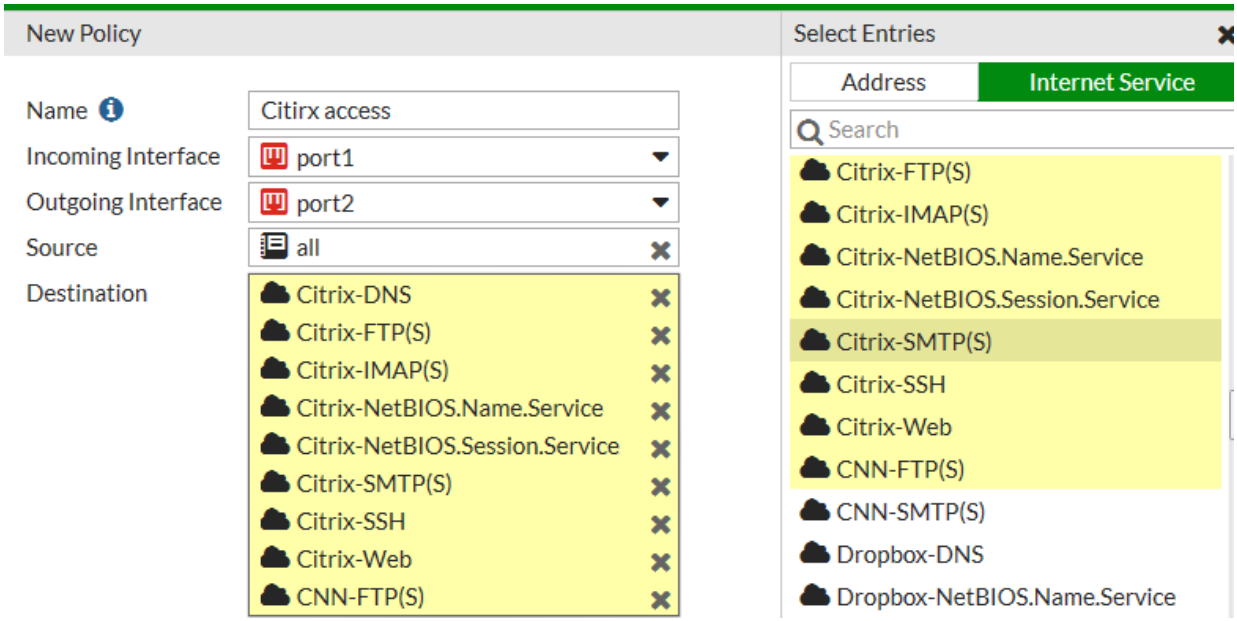
The related CLI options/syntax are:

```
config firewall policy
   edit 1
      set internet-service 1 5 10
      set internet-service-custom test
      set internet-service-negate [enable|disable]
   end
```

GUI

In the policy listing page you will notice that is an Internet Service object is used, it will be found in both the ***Destination*** and ***Service*** column.

In the policy editing page the ***Destination Address***, now ***Destination*** field now has two types, ***Address*** and ***Internet Service***.



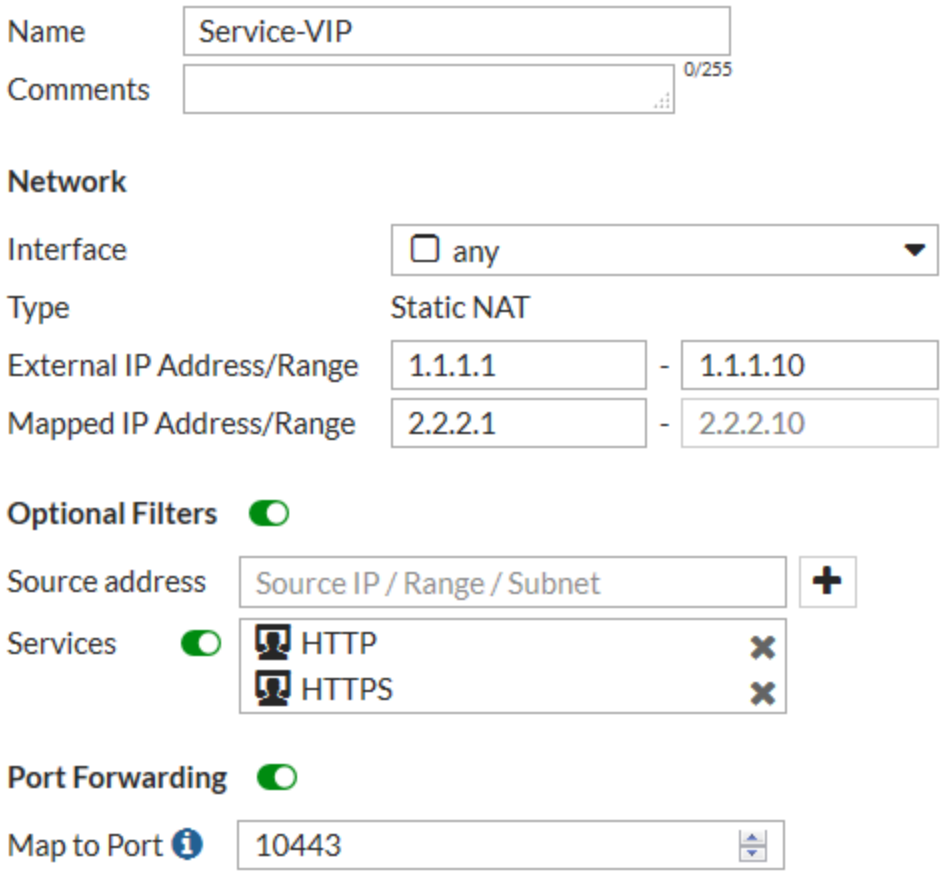
Combining source and destination NAT in the same policy (388718)

The Service field has been added to Virtual IP objects. When `service` and `portforward` are configured, only a single mapped port can be configured. However, multiple external ports can be mapped to that single internal port.

```
config firewall vip
   edit "vip1"
      set type load-balance
      set service "HTTP-8080" "HTTP" <----- New Service field, accepts Service/Service
          group names
      set extip 20.0.0.0-20.0.255.255
      set extintf "wan1"
      set portforward enable
      set mappedip "30.0.0.1"
      set mappedport 100 <-------- single port
      end
```

The reason for making this configuration possible is to allow complex scenarios where multiple sources of traffic are using multiple services to connect to a single computer, while requiring a combination of source and destination NAT and not requiring numerous VIPs bundled into VIP groups.

VIPs with different services will considered non-overlapping.


Name
Service-VIP
Comments
0/255
Network
Interface
any
Type
Static NAT
External IP Address/Range
1.1.1.1
-
1.1.1.10
Mapped IP Address/Range
2.2.2.1
-
2.2.2.10
Optional Filters
Source address
Source IP / Range / Subnet
Services
HTTP
HTTPS
Port Forwarding
Map to Port
10443

NP6 Host Protection Engine (HPE) to add protection for DDoS attacks (363398)

NP6 processors now include HPE functionality that can protect networks from DoS attacks by categorize incoming packets based on packet rate and processing cost and applying packet shaping to packets that can cause DoS attacks. You can use the options in the following CLI command to limit the number packets per second received for various packet types by each NP6 processor. This rate limiting is applied very efficiently because it is done in hardware by the NP6 processor.

HPE protection is disable by default. You can use the following command to enable HPE protection for the NP6_0 NP6 processor:

```
config system np6
   edit np6_0
      config hpe
         set type-shaper enable
      end
```

HPE can be enabled and configured separately for each NP6 processor. When enabled, the default configuration is designed to provide basic DoS protection. You can use the following command to adjust the HPE settings in real time if you network is experiencing an attack. For example, the following command allows you to configure HPE settings for np6_0.

```
config system np6
   edit np6_0
      config hpe
         set type-shaping-tcpsyn-max
         set type-shaping-tcp-max
         set type-shaping-udp-max
         set type-shaping-icmp-max
         set type-shaping-sctp-max
         set type-shaping-ipsec-esp-max
         set type-shaping-ip-frag-max
         set type-shaping-ip-others-max
         set type-shaping-arp-max
         set type-shaping-others-max
      end
```

Where:

`type-shaping-tcpsyn-max` applies shaping based on the maximum number of TCP SYN packets received per second. The range is 10,000 to 10,000,000,000 pps. The default limits the number os packets per second to 5,000,000 pps.

`type-shaping-tcp-max` applies shaping based on the maximum number of TCP packets received. The range is 10,000 to 10,000,000,000 pps. The default is 5,000,000 pps.

`type-shaping-udp-max` applies shaping based on the maximum number of UDP packets received. The range is 10,000 to 10,000,000,000 pps. The default is 5,000,000 pps.

`type-shaping-icmp-max` applies shaping based on the maximum number of ICMP packets received. The range is 10,000 to 10,000,000,000 pps. The default is 1,000,000 pps.

`type-shaping-sctp-max` applies shaping based on the maximum number of SCTP packets received. The range is 10,000 to 10,000,000,000 pps. The default is 1,000,000 pps.

`type-shaping-ipsec-esp-max` NPU HPE shaping based on the maximum number of IPsec ESP packets received. The range is 10,000 to 10,000,000,000 pps. The default is 1,000,000 pps.

`type-shaping-ip-frag-max` applies shaping based on the maximum number of fragmented IP packets received. The range is 10,000 to 10,000,000,000 pps. The default is 1,000,000 pps..

`type-shaping-ip-others-max` applies shaping based on the maximum number of other IP packet types received. The range is 10,000 to 10,000,000,000 pps. The default is 1,000,000 pps.

`type-shaping-arp-max` applies shaping based on the maximum number of ARP packet types received. The range is 10,000 to 10,000,000,000 pps. The default is 1,000,000 pps.

`type-shaping-others-max` applies shaping based on the maximum number of other layer 2 packet types received. The range is 10,000 to 10,000,000,000 pps. The default is 1,000,000 pps.

New feature catalog

The following sections list all of the new features in FortiOS 5.6 organized alphabetically by subject area.

Authentication

New authentication features added to FortiOS 5.6.

FortiToken Mobile Push (397912, 408273, 399839, 404872)

FortiToken Mobile push supports two-factor authentication without requiring users to enter a four-digit code to authenticate. Instead they can just accept the authentication request from their FortiToken Mobile app.

A new command has been added under `config system ftm-push` allowing you to configure the FortiToken Mobile Push services server IP address and port number. The Push service is provided by Apple (APNS) and Google (GCM) for iPhone and Android smartphones respectively. This will help to avoid tokens becoming locked after an already enabled two-factor authentication user has been disabled. In addition, FortiOS supports FTM Push when FortiAuthenticator is the authentication server.

CLI syntax

```
config system ftm-push
   set server-ip <ip-address>
   set server-port [1-65535] Default is 4433.
end
```

In addition, FTM Push is supported on administrator login and SSL VPN login for both iOS and Android. If an SSL VPN user authenticates with their token, then logs out and attempts to reauthenticate again within a minute, a new message will display showing "Please wait x seconds to login again." This replaces a previous error/permission denied message.

The "x" value will depend on the calculation of how much time is left in the current time step.

CLI syntax

```
config system interface
   edit <name>
      set allowaccess ftm
   next
end
```

Support V4 BIOS certificate (392960)

FortiOS now supports backwards compatibility between new BIOS version 4 and old BIOS version 3.

New BIOS V4 certificates:

- Fortinet_CA
- Fortinet_Sub_CA
- Fortinet_Factory

Old BIOS V3 certificates:

- Fortinet_CA_Backup
- Fortinet_Factory_Backup

When FortiOS connects to FortiGuard, FortiCloud, FortiManager, FortiAnalyzer, FortiSandbox as a client, the new BIOS certificate **Fortinet_Factory** will be the default client certificate. When the server returns its certificate (chain) back, FortiOS looks up the issuer of the server certificate and either keeps client certificate as is or switches to the old BIOS certificate **Fortinet_Factory_Backup**. This process occurs in one handshake.

When FortiOS connects to FortiCare, the new BIOS certificate **Fortinet_Factory** is the only client certificate and Server Name Indication (SNI) is set. There is no switchover of certificate during SSL handshake.

When FortiOS acts as a server when connected by FortiExtender, FortiSwitch, FortiAP, etc., **Fortinet_Factory** is the default server certificate. FortiOS detects SNI in client hello, and if no SNI is found or if the CN in SNI is different from the CN of **Fortinet_CA**, it switches to use the old **Fortinet_Factory_Backup**.

Support extendedKeyUsage for x.509 certificates (390393)

As per Network Device Collaborative Protection Profile (NDcPP) v1.0 requirements, server certificates used for TLS connections between FortiGate and FortiAnalyzer should have the "Server Authentication" and "Client Authentication" extendedKeyUsage fields in FIPS/CC mode.

To implement this, a new CLI command has been added under `log fortianalyzer setting` to allow you to specify the certificate used to communicate with FortiAnalyzer.

CLI syntax

```
config log fortianalyzer setting
   set certificate <name>
end
```

Administrator name added to system event log (386395)

The administrator's name now appears in the system event log when the admin issues a user quarantine ban on a source address.

Support RSA-4096 bit key-length generation (380278)

In anticipation of quantum computers, RSA-4096 bit key-length CSRs can now be imported.

New commands added to config user ldap to set UPN processing method and filter name (383561)

Added two new commands to `config user ldap` allowing you to keep or strip domain string of UPN in the token as well as the search name for this kind of UPN.

CLI syntax:

```
config user ldap
   set account-key-processing
   set account-key-name
```

```
end
```

User authentication max timeout setting change (378085)

To accommodate wireless hotspot users authenticated on the FortiGate, the user authentication max timeout setting has been extended to three days (from one day, previously).

Changes to Authentication Settings > Certificates GUI (374980)

Added new icons for certificate types and updated formatters to use these new icons.

Password for private key configurable in both GUI and CLI (374593)

FortiOS 5.4.1 introduced a feature that allowed you to export a local certificate and its private key in password protected p12, and later import them to any device. This option to set password for private key was available only in the CLI (when requesting a new certificate via SCEP or generating a CSR). This feature is now also configurable through the GUI.

The new **Password for private key** option is available under **System > Certificates** when generating a new CSR.

RADIUS password encoding (365145)

A new CLI command, under `config user radius`, has been added to allow you to configure RADIUS password encoding to use ISO-8859-1 (as per RFC 2865).

Certain RADIUS servers use ISO-8859-1 password encoding instead of others such as UTF-8. In these instances, the server will fail to authenticate the user, if the user's password is using UTF-8.

CLI syntax

```
config user radius
   edit <example>
      set password-encoding <auto | ISO-8859-1>
end
```

This option will be skipped if the `auth-type` is neither `auto` nor `pap`.

RSSO supports Delegated-IPv6-Prefix and Framed-IPv6-Prefix (290990)

Two attributes, **Delegated-IPv6-Prefix** and **Framed-IPv6-Prefix**, have been introduced for RSSO to provide a /56 prefix for DSL customers. All devices connected from the same location (/56 per subscriber) can be mapped to the same profile without the need to create multiple /64 or smaller entries.

Device identification

New Device Identification features added to FortiOS 5.6.

Changed default for device-identification-active-scan to disabled (380837)

It was decided that most customers would not appreciate a default setting that resulted in the FortiGate probing their systems, so active scan option is changed to disabled by default going forward, but upgrade code is added to keep the option enabled for those upgrading from 5.4.0 or 5.4.1 who were using device-identification with active scan enabled.

Diagnose command changes

New diagnose features added to FortiOS 5.6.

Add missing "diag npu np6 ..." Commands (305808)

The following `diag npc np6` commands have been reintroduced into 5.6.0.

These options were available in 5.2.x but were not in 5.4.0

- `diag npc np6 gmac-stats` - Shows the GMAC MIBs counters
- `diag npc np6 gmac-stats-clear` - Clears the GMAC MIBS counters
- `diag npc np6 gige-port-stats` - Shows the GIGE PORT MIBs counters
- `diag npc np6 gige-port-stats-clear` - Clears the GIGE PORT MIBs counters

Diagnose command to show firewall service cache (355819)

A diagnostic command has been added to dump out the service name cache kept by the `miglogd` daemon for each individual VDOM.

```
diag test app miglogd 106
```

Example output:

This output has been edited down to conserve space. Only the first 5 of each grouping has been included.

```
diag test app miglogd 106
tcp
port(0), name(NONE)
port(21), name(FTP)
port(22), name(SSH)
port(23), name(TELNET)
port(25), name(SMTP)
udp
port(53), name(DNS)
port(67--68), name(DHCP)
port(69), name(TFTP)
port(88), name(KERBEROS)
port(111), name(ONC-RPC) extra: (ONC-RPC) (NFS)
icmp
port(1), name(test)
port(8), name(PING)
port(13), name(TIMESTAMP)
port(15), name(INFO_REQUEST)
port(17), name(INFO_ADDRESS)
general
prot(6), port(4300), name(example.com_Webadmin)
prot(6), port(5060), name(SIP)
prot(6), port(5190--5194), name(AOL)
prot(6), port(5631), name(PC-Anywhere)
prot(6), port(5900), name(VNC)
service names:
```

```
WINFRAME,DNS,DCE-RPC,H323,RLOGIN,IRC,UUCP,example.com_Webadmin,HTTPS,WAIS,FINGER,REXEC,
RAUDIO,SNMP,TIMESTAMP,RADIUS-OLD,DHCP,AOL,MGCP,SMTPS,INFO_REQUEST,HTTP,SCCP,SOCKS,PPTP,
ONC-RPC,NNTP,SMTP,QUAKE,PC-Anywhere,TFTP,NONE,SSH,RSH,IMAPS,LDAP_UDP,SIP,RIP,PING,PING6,
X-WINDOWS,SMB,SAMBA,TRACEROUTE,NFS,WINS,L2TP,IMAP,GOPHER,SIP-MSNmessenger,SYSLOG,DHCP6,
TELNET,LDAP,MS-SQL,MMS,KERBEROS,SQUID,NTP,FTP,CVSPSERVER,test,AFS3,POP3,Internet-Locator-
    Service,
service groups:
Email Access(DNS,IMAP,IMAPS,POP3,POP3S,SMTP,SMTPS,)
Windows AD(DCE-RPC,DNS,KERBEROS,LDAP,LDAP_UDP,SAMBA,SMB,)
Web Access(DNS,HTTP,HTTPS,)
Exchange Server(DCE-RPC,DNS,HTTPS,)
policies involving multiple service definitions:
```

Diagnose command to show crash history and adjust crash interval (366691)

In order to alleviate the impact logging put on resources if processes repeatedly crash, limits have been put on crash logs.

- The default limit is 10 times per 60 minutes for crash logs. This limit can be edited using the command:

  ```
  diagnose debug crashlog interval <interval>
  ```

  `<interval>` is the number of second to log crash logs for a particular process

- The `miglogd` daemon is the only one to write crash logs directly. Crash logs from other processes are done through miglogd.
- Crash logs for a single crash are written all at once so that the logs are easier to read if there are crashes of multiple processes at the same time.
- A diagnose command has been added to show crash history.

  ```
  # diagnose debug crashlog history
  # Crash log interval is 3600 seconds
  # reportd crashed 2 times. The latest crash was at 2016-12-01 17:53:45
  ```

diagnose switch-controller commands (368197)

The following diagnose commands in the CLI, are designed to

- Output stats on the managed switches
- Kick the client from the managed switches

```
diagnose switch-controller dump lldp neighbors-summary <device-id> <portid>
diagnose switch-controller dump lldp neighbors-detail <device-id> <portid>
diagnose switch-controller dump lldp Stats <device-id>
diagnose switch-controller dump port-stats <device-id>
diagnose switch-controller dump trunk-state <device-id>
diagnose switch-controller kick <device-id> <vlan ID> <port ID> <MAC ID>
```

While not a diagnostic command, the following can also be run from VDOMs

```
execute replace-device fortiswitch <device-id>
```

These commands are now longer restricted to being run from the root VLAN and can be run from any VDOM

Diagnose commands for monitoring NAT sessions (376546)

We have developed the following monitoring capabilities in CLI and SNMP.

- NAT sessions per IP pool
- Total tcp sessions per IP pool
- Total udp sessions per IP pool
- Total others (non-tcp and non-udp) sessions per IP pool

FortiGate supports 4 types of NAT, which are

- Overload
- One-to-one
- Fixed-port-range
- Port-block-allocation.

diagnose firewall ippool-all

- list - lists all of the IP Pools
- stats - Statistics of the IP Pools

list

```
diagnose firewall ippool-all list
```

Example output:

```
vdom:root owns 4 ippool(s)
name:Client-IPPool
type:port-block-allocation
nat-ip-range:10.23.75.5-10.23.75.200
name:Fixed Port Range
type:fixed-port-range
nat-ip-range:20.20.20.5-20.20.20.50
name:One to One
type:one-to-one
nat-ip-range:10.10.10.5-10.10.10.50
name:Sales_Team
type:overload
nat-ip-range:10.23.56.18-10.23.56.20
```

Stats

This option has two methods of being used. By just hitting enter after stats, the output contains the stats for all of the IP Pools. By putting the name of an IP Pool after stats, the output is filtered so that only stats relating to that particular IP Pool is included in the output.

Example output #1

```
# diagnose firewall ippool-all stats
vdom:root owns 5 ippool(s)
name: Client-IPPool
```

```
type: port-block-allocation
startip: 10.23.75.5
endip: 10.23.75.200
total ses: 0
tcp ses: 0
udp ses: 0
other ses: 0
name: Fixed Port Range
type: fixed-port-range
startip: 20.20.20.5
endip: 20.20.20.50
total ses: 0
tcp ses: 0
udp ses: 0
other ses: 0
name: One to One
type: one-to-one
startip: 10.10.10.5
endip: 10.10.10.50
total ses: 0
tcp ses: 0
udp ses: 0
other ses: 0
name: Sales_Team
type: overload
startip: 10.23.56.18
endip: 10.23.56.20
total ses: 0
tcp ses: 0
udp ses: 0
other ses: 0
```

Example #2

```
# diagnose firewall ippool-all stats "Sales_Team"
name: Sales_Team
type: overload
startip: 10.23.56.18
endip: 10.23.56.20
total ses: 0
tcp ses: 0
udp ses: 0
other ses: 0
```

SIP diagnose command improvements (376853)

A diagnose command has been added to the CLI that outputs VDOM data located in the voipd daemon.

```
diagnose sys sip-proxy vdom
```

Example

```
(global) # diagnose sys sip-proxy vdom
VDOM list by id:
vdom 0 root (Kernel: root)
vdom 1 dmgmt-vdom (Kernel: dmgmt-vdom)
vdom 2 test2 (Kernel: test2)
```

```
vdom 3 test3 (Kernel: test3)
vdom 4 vdoma2 (Kernel: vdoma2)
vdom 5 vdomb2 (Kernel: vdomb2)
vdom 6 vdomc2 (Kernel: vdomc2)
vdom 7 vdoma (Kernel: vdoma)
vdom 8 vdomb (Kernel: vdomb)
vdom 9 vdomc (Kernel: vdomc)
VDOM list by name:
vdom 1 dmgmt-vdom (Kernel: dmgmt-vdom)
vdom 0 root (Kernel: root)
vdom 2 test2 (Kernel: test2)
vdom 3 test3 (Kernel: test3)
vdom 7 vdoma (Kernel: vdoma)
vdom 4 vdoma2 (Kernel: vdoma2)
vdom 8 vdomb (Kernel: vdomb)
vdom 5 vdomb2 (Kernel: vdomb2)
vdom 9 vdomc (Kernel: vdomc)
vdom 6 vdomc2 (Kernel: vdomc2)
```

Diagnose command to get AV virus statistics (378870)

A new diagnostic command has been added for the showing of AV statistics. This can be used within each VDOM

Syntax:

```
diagnose ips av stats show
```

Example output

```
diagnose ips av stats show
AV stats:
HTTP virus detected: 0
HTTP virus blocked: 0
SMTP virus detected: 0
SMTP virus blocked: 0
POP3 virus detected: 0
POP3 virus blocked: 0
IMAP virus detected: 0
IMAP virus blocked: 0
NNTP virus detected: 0
NNTP virus blocked: 0
FTP virus detected: 0
FTP virus blocked: 0
SMB virus detected: 0
SMB virus blocked: 0
```

Diagnose command to get remote FortiSwitch trunk information (379329)

To ensure that a FortiGate and its managed FortiSwitches stay in synchronization in the event of an inadvertent trunk table change situation, there is a new CLI setting that checks for discrepancies.

The idea is to check to see if there will be a synchronization issue between the FortiGate and the FortiSwitch before applying the configuration

1. On fortilink reconnection, FGT reads trunk table of FSW using REST API GET-- Hence FGT gets all the port and its trunk membership information from FSW

2. FGT then compares its managed FSW trunk information with received FSW information
3. If there is any conflict, FGT will delete extra/conflicted trunk on FSW using REST API POST
4. At the end FGT replays all configuration to FSW as usual

This will help delete the extra trunks, conflicted trunks on the FSW and to make sure in sync

Possible reasons for losing synchronization include:

- The FortiGate reboots after a factory reset while there is still a trunk configuration in the FortiSwitch.
- The managed FortiSwitch's trunk table gets edited on the FortiGate while the FortiSwitch is offline.
- A trunk table on the FortiSwitch gets added or the existing one gets modified or deleted by a user.

New diagnose command for the CLI:

```
diagnose switch-controller dump trunk-switch-config <Managed FortiSwitch device ID>
```

help provided for diagnose debug application csfd (379675)

The syntax for the command is:

```
diagnose debug application csfd <Integer>
```

The <Integer> being the debug level. To get the integer value for the debug level, run the command without the integer. You will get the following:

```
# diagnose debug application csfd
csfd debug level is 0 (0x0)
Error 0x01
Warning 0x02
Function trace 0x04
Information 0x08
Detail 0x10
MAC packet encryption debug 0x20
MAC learning debug 0x40
FAZ configuration synchronize debugging 0x0080
FAZ configuration function trace 0x00100
Configuration tree update debug 0x00200
Configuration tree function trace 0x00400
HA Sync plugin debug 0x00800
```

Convert the value next to the debug level you want to an integer. For example, to set the debug level to `Information`, convert `0x08` to `8` and use it for the option at the end of the command.

```
# diagnose debug application csfd 8
```

New IPS engine diagnose commands (381371)

Periodically, when troubleshooting, an different IPS engine will need to be installed on the FortiGate but there will also be a restriction that the FortiGate can't be rebooted. Normally, a new IPS engine will not be fully recognized by the system until after a reboot. This command allows the running of new commands or new versions of commands in the IPS engine without having to reboot the FortiGate.

```
diagnose ips test cmd <command strings>
```

The command strings are separated by a semicolon such as:

```
diagnose ips test cmd command1;command2;command3
```

Examples:

- `diagnose ips test cmd "ips session status"`

  This command triggers the diagnosis command in the double quotation marks: "diagnose ips session status"

- `diag ips test cmd "ips memory track; ips memory status; ips session status"`

  This command triggers the diagnosis commands in the double quotation marks in order.

  The results:

```
Commands[0]: ips memory track
----< execute "diagnose ips memory track" >----
Commands[1]: ips memory status
----< execute "diagnose ips memory status" >----
Commands[2]: ips session status
----< execute "diagnose ips session status" >----
```

New AV engine diagnose commands (383352)

The purpose of this diagnostic command is to display information from within the AV engine for the purposes of aiding trouble shooting and diagnostics if the AV engine crashes or times out.

The command is:

```
diagnose antivirus test
```

It's syntax can be one of the following:

```
diagnose antivirus test <command>
diagnose antivirus test <command argument1>; <argument2>; ...
```

The command is defined and interpreted by the AV engine. FortiOS just passes the CLI

command into the AV engine and outputs the strings returned by AV engine.

In AV engine 5.4.239, the following command are supported.

- `get scantypes`
- `set scantypes`
- `debug`

NPU diagnose command now included HPE info in results (384692)

There is now change to the CLI but the results of the `diagnose npu np6 npu-feature` command now include results regarding HPE.

clear checksum log files (diag sys ha checksum log clear) (385905)

There is currently a command, `diag sys ha checksum log [enable | disable]` that enables a checksum debug log by saving checksum calculations to a temp file. However, the checksum calculations saved

in this file can be processed by two different functions, `cmdbsvr` and the CLI.

The function `cmf_context-is-server()` now enables the determining whether the running process is `cmdbsvr` or the CLI and also a diagnose command has been added to clear the contents of the file.

```
diag sys ha checksum log clear
```

new diagnose command to delete avatars (388634)

It is now possible to delete avatars associated with FortiClient clients.

```
diagnose endpoint avatar delete <FortiClient UID>
```

or

```
diagnose endpoint avatar delete <FortiClient UID> <username>
```

- If only the FortiClient UID is used, all of the avatars, except those that are currently being used will be deleted.
- If both the FortiClient UID and the username are used, all of the avatars that belong to that combination, except those being used, will be deleted.

CID signatures have been improved for DHCP and CDP (389350, 409436)

More parameters have been added to make them more specific. This helps to reduce false positives.

- DHCP signatures:
  - A new dhcp signature file has been added 'cid.dhcp2' that allows for the class and host name to specified in the same signature. This is for increased accuracy.
  - Relevant signatures from 'cid.dhcp' have been ported to the new signature file 'cid.dhcp2'
  - Support DHCP parameter matching in signatures.
  - Support DHCP option list matching in signatures.
- CDP mac analyzer now passes all three keys to the OS matcher.
- Tests:
  - A number of new tests (including pcaps) have been added to match existing signatures and new signatures.
  - Some tests where multiple protocols were present in a single pcap, have been modified. These are now split into multiple pcaps, each containing a single protocol. This allows FortiOS to fully test a signature, where previously a single test may have matched multiple signatures.
- CID debug statistics now use shared memory. This prevents the daemon from having to respond to CLI requests and allows for the stats to persist across daemon restarts.
  - A Change has been made to the host ip update priority. IP changes for routers that have had their type set by heuristic are not allowed to change IPs.
  - If it is a Fortinet device, the change is allowed if it comes through a protocol we trust more (CDP, DHCP, LLDP, or MAC).

diagnose command to calculate socket memory usage (392655)

This diagnostic command gives the socket memory usage by individual process.

```
diagnose sys process sock-mem <pid>; <pid> ...
```

Separate arguments with a semicolon ";"

Example

Run diagnose sys top to get the pid of a few process...

```
diagnose sys top
Run Time: 1 days, 0 hours and 44 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 7996T, 5839F
httpsd  214 S 0.1 0.2
httpsd 1398 S 0.1 0.2
snmpd  173 S 0.1 0.1
```

Then use those pid with the command...

```
diagnose sys process sock-mem 214; 173
Process ID=214, sock_mem=0(bytes)
Process ID=173, sock_mem=2(bytes)
```

FortiGuard can determine a FortiGate's location from its public IP address (393972)

The FortiGate now shows the public IP address and the geographical location (country) in the dashboard. The FortiGate sends a ping to the FortiCare/FortiGuard network and as a response receives the local WAN IP, or if it is being NATed the public IP of the network. Using the public IP address a geo-ip Blackpool is done to determine the country.

In the same location on the Dashboard, it also shows whether or not the listed IP address if a member of the Fortinet Blacklist.

CLI

The diagnostic command to get the information is:

```
diag sys waninfo
```

Example:

```
diagnose sys waninfo
Public/WAN IP: 209.87.240.98
Location:
Latitude: 45.250100
Longitude: -75.916100
Accuracy radius: 5
Time zone: America/Toronto
City: Stittsville
Subdivisions:
0: Ontario
Country: Canada
Postal:
Code: K2S
Continent: North America
Registered country: Canada
ISP: Unknown

Failed to query whether 209.87.240.98 is in the FortiGuard IP Blacklist: ret=-1 buf_
    sz=1024
```

```
Command fail. Return code 5
```

To get information about the address's inclusion as a member of the Fortinet Blacklist, the command is:

```
diag fortiguard ipblacklist [db | vr | ip | ctx]
```

- `db` - Get Database and Vendor/Reason List Versions.
- `vr` - Get Vendor/Reason List.
- `ip` - Get Information on Specific IP.
- `ctx` - Show Local Context.

If using the ip option, specify the IPv4 address after the ip option.

Example:

```
diagnose fortiguard ipblacklist ip 209.87.240.98
```

AWS bootstrapping diagnose commands (394158)

Bootstrap feature is quite similar to cloudinit in Openstack. When user launching a new instance of FGT-VM in AWS, it needs to provide some basic information of license and config stored in AWS s3 bucket via userdata. Bootstrap will download license and config from s3 bucket and apply them to FGT automatically.

CLI

Add a new cli to show the results of bootstrap config apply.

Example:

```
diagnose debug aws-bootstrap show
>> FGVM040000066475 $ config sys glo
>> FGVM040000066475 (global) $ set hostname awsondemand
>> FGVM040000066475 (global) $ end
```

Diagnose command to aid in conserver mode issues (394856)

The `diagnose hardware sys conserve` command provides memory information about the system that is useful in diagnosing conserve mode issues.

Example

```
diagnose hardware sys conserve
memory conserve mode: off
total RAM: 7996 MB
memory used: 2040 MB 25% of total RAM
memory used threshold extreme: 7597 MB 95% of total RAM
memory used threshold red: 7037 MB 88% of total RAM
memory used threshold green: 6557 MB 82% of total RAM
```

Diagnose commands to display FortiCare registration information (395254)

The Dashboard License widget can display information about the registered company owner and industry. There are some diagnostic commands that can do that in the CLI.

```
diagnose forticare protocol [HTTP | HTTPS]
```

```
diagnose forticare server < server IP>
diagnose forticare cnreg-code-list - List of known ISO 3166-1 numeric country/region
    codes.
diagnose forticare direct-registration reseller-list <cnreg-code>
diagnose forticare direct-registration country-data <cnreg-code>
diagnose forticare direct-registration organization-list
diagnose forticare direct-registration product-registration <arguments>
```

Options/arguments for product registration:

- a = account_id
- A = address
- y = city
- C = company
- c = contract_number
- T = country_code
- e = existing_account
- F = fax
- f = first_name
- h = help
- I = industry
- i = industry_id
- l = last_name
- O = orgsize
- o = orgsize_id
- p = password
- P = phone
- z = postal_code
- R = reseller
- r = reseller_id
- S = state
- s = state_code
- t = title
- v = version

new diag test app csfd options (395302)

Two additional test levels have been added to the `diag test app csfd` command in order to dump some additional information about timers, file handlers status and received MAC addresses to the HA master.

```
diag test app csfd 11
diag test app csfd 40
```

new 'AND' and 'OR' filter capabilities for debug flow addr (398985)

In order to make a more flexible filter for the debug flow address command, the Boolean arguments of 'AND' and 'OR' have been added to the command parser. This will work regardless of whether or not the source or destination address is being filtered.

Syntax:

```
diagnose debug flow filter address <IP1|from IP> <IP2|to IP> <ENTER|and/or>
```

Improve wad debug trace and crash log information (400454)

Previously, when filtering on a wad debug trace or crash log information, the information may not have been as targeted as necessary. A new setting has been added to target a specific policy.

```
diagnose wad filter firewall-policy <index>
diagnose wad filter explicit-policy <index>
```

These commands will target the firewall or explicit proxy policies. Using a "`-1`" as the value will index of that particular policy type.

diag sys sip-proxy config profile --> diag sys sip-proxy config profiles (404874)

Diagnose command has been changed to make it more consistent with other similar commands.

```
diagnose system sip-proxy config profile
```

has been changed to

```
diagnose system sip-proxy config profiles
```

diag debug flow changes (405348)

For crash and console logs, the logs are no longer parsed before being sent to their destination. Now they are dumped directly to the destination.

In addition the following options have been removed from the diagnose command list:

```
diag debug flow show console
diag debug flow show console enable
diag debug flow show console disable
```

improve wad memory diagnose process (408236)

The WAD SSL memory dump functions have been moved to migbase so they can be shared by both WAD and CLI.

CLI additions

- `diagnose wad memory` - WAD memory diagnostics
- `diagnose wad memory general` - List of WAD memory blocks.

- `diagnose wad memory bucket` List suspicious WAD memory buckets.
- `diagnose wad memory ssl` List SSL memory statistics

New daemon watchdog framework in forticron (409243)

A new feature has been added to dump userspace's process stacks.

CLI additions:

```
diagnose sys process pstack <pid>
```

`<pid>` - Process ID, such as those displayed when using `diagnose sys top`

DNS log improvements (410132)

DNS logs have been improved to make the presentation of the data clearer. These changes involve a reorganization of the DNS log subtypes.

These changes include:

- Change `dns-subtype` to `dns-response`
- Remove `status` field and add Pass/Block/Redirect to `action` field
- Change the `msg` field display DNS filter rating results
- All error messages now to the `error` field
- Change `urlfilteridx` to `domainfilteridx`
- Change `urlfilterlist` to `domainfilterlist`
- Add a query type value field.

Explicit web proxy

New explicit web proxy features added to FortiOS 5.6.

Explicit proxy supports multiple incoming ports and port ranges (402775, 398687)

Explicit proxy can now be configured to listen on multiple ports on the same IP as well as listen for HTTP and HTTPS on those same (or different) ports.

Define the IP ranges using a hyphen (**-**). As shown below, `port_high` is not necessary to specify if `port_low` is equal to `port_high`.

CLI syntax

```
config web-proxy explicit
   set http-incoming-port <port_low> [-<port_high>]
end
```

Explicit proxy supports IP pools (402221)

Added a new command, `poolname`, to `config firewall explicit-proxy-policy`. When setting the IP pool name with this command, the outgoing IP will be selected.

CLI syntax

```
config firewall explicit-proxy-policy
   edit <example>
      set poolname <name>
end
```

Option to remove unsupported encoding from HTTP headers (392908)

Added a new command to `config web-proxy profile` that, when enabled, allows the FortiGate to strip out unsupported encoding from request headers, and correctly block banned words. This is to resolve issues when attempting to successfully block content using Google Chrome.

CLI syntax:

```
config web-proxy profile
   edit <example>
      set strip-encoding {enable | disable}
end
```

New authentication process for explicit web proxying (386474, 404355)

While in Proxy inspection mode, explicit proxy options can be set under **Network > Explicit Proxy**. These settings will affect what options are available for creating proxy policies under **Policy & Objects > Proxy Policy**. From here you may create new policies with **Proxy Type** set to either **Explicit Web**, **Transparent Web**, or **FTP**.

Authentication will be triggered differently when configuring a transparent HTTP policy. Before such a policy can be configured, you must enable **HTTP Policy Redirect** under **Security Profiles > Proxy Options**.

Added Internet services to explicit proxy policies (386182)

Added two new commands to `config firewall explicit-proxy-policy`. FortiOS can use the Internet Service Database (introduced in 5.4.1) as the web-proxy policy matching factor.

CLI syntax:

```
config firewall explicit-proxy-policy
   edit <example>
      set internet-service <application-id>
      set internet-service-custom <application-name>
```

Virtual WAN link in an explicit proxy firewall policy (385849, 396780)

Virtual WAN link (VWL) interfaces may now be set as the destination interface in an explicit proxy policy, routing traffic properly using basic virtual WAN link load balance settings. This is now configurable through both the CLI under `firewall explicit-proxy-policy` and the GUI.

Added application ID and category setting on the explicit proxy enabled service (379330)

This feature introduces support for application ID/category in the service of explicit proxy as one policy selection factor. The intent is to identify the application type based on the HTTP request with IPS application type detection function. It is similar to the current firewall explicit address, but it is implemented as a service type, and you can select the application ID/ category to define explicit service. Of course, now it must be an HTTP-based application.

CLI syntax

```
config firewall service custom
   edit "name"
      set app-service-type [disable|app-id|app-category]
   next
end
```

Explicit Proxy - populate pac-file-url in transparent mode (373977)

You can now use manageip to populate pac-file-url in transparent opmode. Previously, in the CLI, when displaying pac-file-url, the code only tries to get interface IP to populate pac-file-url.

CLI syntax

```
config vdom
   edit root
   config system settings
      set opmode transparent
      set manageip 192.168.0.34/24
end
   config web-proxy explicit
      set pac-file-server-status enable
      get pac-file-url [url.pac]
```

```
end
```

SSL deep inspection OCSP support for Explicit Proxy (365843)

OCSP support for SSL deep inspection added for Explicit Proxy.

CLI syntax

```
config vpn certificate setting
   set ssl-ocsp-status [enable|disable]
   set ssl-ocsp-option [certificate|server]
end
```

Timed out authentication requests are now logged (357098)

CLI syntax

```
config web-proxy explicit
   set trace-auth-no-rsp [enable|disable]
end
```

Firewall

New firewall features added to FortiOS 5.6.

Optimization of the firewall Service cache (355819)

In order to improve the efficiency and performance of the firewall Service cache, the following improvements have been made:

- The logic behind the structure of the cache has been simplified. Instead of storing ranges of port numbers, we store each individual port number in the cache
- Separate caches are created for each VDOM so that cache searches are faster.
- The performance of more frequently used cases has been increased
- Hash tables are used to improve the performance of complex cases. These could include such instances as:
  - service names tied to specific IP Ranges
  - redefinition (one port number with multiple service names)

New CLI option to prevent packet order problems for sessions offloaded to NP4 or NP6 (365497)

In order to prevent the issue of a packet, on FortiGate processing a heavy load of traffic, from being processed out of order, a new setting has been added to better control the timing of pushing the packets being sent to NP units.

The new option, delay-tcp-npc-session, has been added into the context of config firewall policy within the CLI

```
config firewall policy
   edit <Integer for policy ID>
      set delay-tcp-npc-session
      end
```

Policy may not be available on units not using NP units.

GUI changes to Central NAT (371516)

The Central NAT configuration interface prevents the accidental occurrence of being able to select “all” and “none” as two objects for the same field. It only allows the selecting of a single IP pool, though it is still possible to select multiple IP pools within the CLI.

Max value for Firewall User authentication changed (378085)

Previously, the maximum time that a member of a firewall user group could remain authenticated without any activity was 24 hours (1440 minutes). The maximum value for this setting has been changed to 72 hours (4320 minutes). This allow someone to log in but not be kicked off the system due to inactivity over the course of a weekend.

The syntax in the CLI for configuring this setting is:

```
config user group
   edit <name of user group>
```

```
set authtimeout 4320
end
```

Changes to default SSL inspection configuration (380736)

SSL is such a big part of normal traffic that SSL certificate inspection is no longer disabled by default. SSL inspection is not mandatory in both the CLI and GUI when it is applicable. The default setting is the Certificate Inspection level. As a result there have been a few changes within the CLI and the GUI.

CLI

The setting SSL-SSH-Profile, is a required option, with the default value being “certificate-inspection”, when it is applicable in the following tables:

- firewall.profile-group
- firewall.policy
- firewall.policy6,
- firewall.explicit-proxy-policy

The following default profiles are read-only:

- certificate-inspection
- deep-ssl-inspection

GUI

IPv4/IPv6 Policy and Explicit Proxy Policy edit window

- The configuration and display set up for SSL/SSH Inspection is now similar to "profile-protocol-option" option
- The disable/enable toggle button is no longer available for the Profile Protocol Option
- The default profile is set to "certificate-inspection"

IPv4/IPv6 Policy, Explicit Proxy Policy list page

- There is validation for SSL-SSH-Profile when configuring UTM profiles

SSL/SSH Inspection list page

- There is no delete menu on GUI for default ssl profiles
- The "Edit" menu has been changed to "View" for default SSL profiles
- The default SSL profile entries are considered an implicit class and are grayed out

SSL/SSH Inspection edit window

- The only input for default SSL profiles is now download/view trusted certificate links
- To return to the List page from default SSL profiles, the name of the button is now "Return"

Profile Group edit window

- There is no check box for SSL-SSH-Profile. It is always required.

Add firewall policy comment field content to log messages (387865)

There has been a need by some customer to have some information in the logs that includes specific information about the traffic that produced the log. The rather elegant solution is that when the log-policy-comment option is

enabled, the comment field from the policy will be included in the log. In order to make the logs more useful regarding the traffic just include a customized comment in the policy and enable this setting.

Syntax

```
config system settings
   set log-policy-comment [enable | disable]
   end
```

- This setting is for all traffic and security logs.
- It can be select on a per VDOM basis

Learning mode changes profile type to single (387999)

The Learning mode does not function properly when it is applied to a policy that has a UTM profile group applied to it. The logging that should be taking place from the Learning Mode profiles does not occur as intended, and the

Automatically switching the profile type to single on a policy with Learning mode enabled prevents it from being affected by the UTM policy groups.

MAC address authentication in firewall policies and captive portals (391739)

When enabled, a MAC authentication request will be sent to `fnbamd` on any traffic. If the authentication receives a positive response, login becomes available. If the response is negative the normal authentication process takes over.

CLI

New option in the firewall policy setting

```
config firewall policy
   edit <policy ID>
      set radius-mac-auth-bypass [enable |disable]
      end
```

New option in the interface setting

```
config system interface
   edit <interface>
      set security-mode captive-portal
      set security-mac-auth-bypass
      end
```

Display resolved IP addresses for FQDN in policy list (393927)

If a FQDN address object is used in a policy, hovering the cursor over the icon for that object will show a tool tip that lists the parameters of the address object. This tool tip now includes the IP address that the FQDN resolves to.

Added comment for acl-policy, interface-policy and DoS-policy (396569)

A comment field has been added to the following policy types:

- acl-policy
- interface-policy
- DoS-policy

Comments of up to 1023 characters can be added through the CLI.

Examples:

DoS policy

```
config firewall DoS-policy
   edit 1
      set comment "you can put a comment here(Max 1023)."
      set interface "internal"
      set srcaddr "all"
      set dstaddr "all"
      set service "ALL"
      config anomaly
         edit "tcp_syn_flood"
         set threshold 2000
         next
      end
   end
```

Interface policy

```
config firewall interface-policy
   edit 1
      set comment "you can put a comment here(max 1023)."
      set interface "dmz2"
      set srcaddr "all"
      set dstaddr "all"
      set service "ALL"
      end
```

Firewall ACL

```
config firewall acl
   edit 1
      set status disable
      set comment "you can put a comment here(max 1023)."
      set interface "port5"
      set srcaddr "all"
      set dstaddr "all"
      set service "ALL"
   end
```

Internet service settings moved to more logical place in CLI (397029)

The following settings have moved from the application context of the CLI to the firewall context:

- internet-service
- internet-service-custom

Example of `internet-service`

```
config firewall internet-service 1245324
   set name "Fortinet-FortiGuard"
   set reputation 5
   set icon-id 140
   set offset 1602565
      config entry
         edit 1
            set protocol 6
            set port 443
            set ip-range-number 27
            set ip-number 80
            next
         edit 2
            set protocol 6
            set port 8890
            set ip-range-number 27
            set ip-number 80
            next
         edit 3
            set protocol 17
            set port 53
            set ip-range-number 18
            set ip-number 31
            next
         edit 4
            set protocol 17
            set port 8888
            set ip-range-number 18
            set ip-number 31
            next
         end
```

Example of `internet-service-custom`

```
config firewall internet-service-custom
   edit "custom1"
      set comment "custom1"
         config entry
            edit 1
               set protocol 6
                  config port-range
                     edit 1
                        set start-port 30
                        set end-port 33
                        next
                     end
                  set dst "google-drive" "icloud"
                  next
               end
            next
         end
```

Example of `get` command:

```
get firewall internet-service-summary
Version: 00004.00002
Timestamp: 201611291203
Number of Entries: 1349
```

Certificate key size selection (397883)

FortiOS will now support different SSL certificate key lengths from the HTTPS server. FortiOS will select a key size from the two options of 1024 and 20148, to match the key size (as close as possible, rounding up) on the HTTS server. If the size of the key from the server is 512 or 1024 the proxy will select a 1024 key size. If the key size from the servers is over 1024, the proxy will select a key size of 2048.

CLI changes:

In `ssl-ssh-profile` remove:

- `certname-rsa`
- `certname-dsa`
- `certname-ecdsa`

In `vpn certificate setting`, add the following options :

- `certname-rsa1024`
- `certname-rsa2048`
- `certname-dsa1024`
- `certname-dsa2048`
- `certname-ecdsa256`
- `certname-ecdsa384`

AWS API integration for dynamic firewall address object (400265)

Some new settings have been added to the CLI that will support instance information being retrieved directly from the AWS server. The IP address of a newly launched instance can be automatically added to a certain firewall address group if it meets specific requirements. The new address type is:ADDR_TYPE_AWS

New CLI configuration settings:

The AWS settings

```
config aws
   set access-key
   set secret-key
   set region
   set vpc-id
   set update-interval
```

- `access-key` - AWS access key.
- `secret-key` - AWS secret key.
- `region` - AWS region name.
- `vpc-id` - AWS VPC ID.
- `update-interval` - AWS service update interval (60 - 600 sec, default = 60).

The AWS address:

```
config firewall address
   edit <address name>
      set type aws
      set filter <filter values>
```

The filter can be a combination of any number of conditions, as long as the total length

of filter is less than 2048 bytes. The syntax for the filter is:

```
<key1=value1> [& <key2=value2>] [| <key3=value3>]
```

For each condition, it includes a key and value, the supported keys are:

1. `instanceId`, (e.g. instanceId=i-12345678)
2. `instanceType`, (e.g. instanceType=t2.micro)
3. `imageId`, (e.g. imageId=ami-123456)
4. `keyName`, (e.g. keyName=aws-key-name)
5. `architecture`, (e.g. architecture=x86)
6. `subnetId`, (e.g. subnetId=sub-123456)
7. `placement.availabilityzone`, (e.g. placement.availabilityzone=us-east-1a)
8. `placement.groupname`, (e.g. placement.groupname=group-name)
9. `placement.tenancy`, (e.g. placement.tenancy=tenancy-name)
10. `privateDnsName`, (e.g. privateDnsName=ip-172-31-10-211.us-west-2.compute.internal)
11. `publicDnsName`, (e.g. publicDnsName=ec2-54-202-168-254.us-west-2.compute.amazonaws.com)
12. AWS instance tag, each tag includes a key and value, the format of tag set is: `tag`.Name=Value, maximum of 8 tags are supported.

Internet service configuration (405518)

To make the CLI configuration of Internet service configuration more intuitive, the settings for Internet service in Explicit Web proxy are closer to those in the Firewall police. An Internet service enable switch has been added to the Explicit Web proxy with the same text description as the Firewall policy.

CLI:

The relevant options in the firewall policy are:

```
config firewall policy
   edit 1
      set internet-service enable
      set internet-service-id 327681 1572864 917519 393225 1572888 1572877 917505
   next
   end
```

The Explicit Web proxy is now has these options:

```
config firewall explicit-proxy-policy
edit 1
set uuid f68e0426-dda8-51e6-ac04-37fc3f92cadf
set proxy web
```

```
set dstintf "port9"
set srcaddr "all"
set internet-service 2686980
set action accept
set schedule "always"
set logtraffic all
next
end
```

Changes to SSL abbreviate handshake (407544)

The SSL handshake process has changed to make troubleshooting easier.

- In order to better identify which clients have caused SSL errors, the WAD SSL log will use the original source address rather than the source address of packets.
- The return value of `wad_ssl_set_cipher` is checked.
- The `wad_ssl_session_match` has been removed because it will add the connection into bypass cache and bypass further inspection.
- DSA and ECDSA certificates are filtered for `admin-server-cert`
- `cert-inspect` is reset after a WAD match to a Layer 7 policy
- An option to disable the use of SSL abbreviate handshake has been added

CLI addition

```
config firewall ssl setting
   set abbreviate-handshake [enable|disable]
```

NGFW mode in the VDOM - NAT & SSL Inspection considerations (407547)

Due to how the NGFW Policy mode works, it can get complicated in the two areas of NAT and SSL Deep Inspection. To match an application against a policy, some traffic has to pass through the FortiGate in order to be properly identified. Once that happens may end up getting mapped to a different policy, where the new policy will be appropriately enforced.

NAT

In the case of NAT being used, the first policy that is triggered to identify the traffic might require NAT enabled for it to work correctly. i.e., without NAT enabled it may never be identified, and thus not fall through. Let's use a very simple example:

Policy 1: Block Youtube

Policy 2: Allow everything else (with NAT enabled)

Any new session established will never be identified immediately as Youtube, so it'll match policy #1 and let some traffic go to try and identify it. Without NAT enabled to the Internet, the session will never be setup and thus stuck here.

Solution:

- NAT for NGFW policies must be done via Central SNAT Map
- Central SNAT Map entries now have options for 'srcintf', 'dstintf' and 'action'.

- If no IP-pools are specified in the Central SNAT entry, then the outgoing interface address will be used.
- NGFW policies now must use a single default ssl-ssh-profile. The default ssl-ssh-profile can be configured under the system settings table.

SSL

In the case of SSL inspection, the issue is a bit simpler. For each policy there are 3 choices:

1. No SSL,
2. Certificate Only
3. Deep Inspection.

For 1. and 2. there is no conflict and the user could enable them inter-changeably and allow policy fallthrough.

The issue happens when:

- The first policy matched, uses ***Certificate Only***
- After the application is detected, it re-maps the session to a new policy which has ***Deep Inspection*** enabled

This switching of behavior is the main cause of the issue.

Solution:

- Multiple SSL profiles have been replaced with a single page of settings
- The user can setup exemptions for destination web category, source IP or etc.

CLI

Changes

```
config system settings
   set inspection-mode flow
   set policy-mode [standard | ngfw]
```

Has been changed to:

```
config system settings
   set inspection-mode flow
   set ngfw-mode [profile-based | policy-based]
```

- `ngfw-mode` - Next Generation Firewall mode.
- `profile-based` - Application and web-filtering is configured using profiles applied to policy entries.
- `policy-based` - Application and web-filtering is configured as policy match conditions.

Additions

Setting the vdom default ssl-ssh-profile

```
config system settings
   set inspection-mode flow
   set ngfw-mode policy-based
   set ssl-ssh-profile <profile>
```

`ssl-ssh-profile` - VDOM SSL SSH profile.

Setting srcintf, dstintf, action on the central-snat policy

```
config firewall central-snat-map
   edit <id>
      set srcintf <names or any>
      set dstintf <names or any>
      set action (permit | deny)
```

- `srcintf` - Source interface name.
- `dstintf` - Destination interface name.
- `action` - Action of central SNAT policy.

GUI

System settings, VDOM settings list/dialog:

- A field has been added to show the default `ssl-ssh-profile`

IPv4/v6 Policy list and dialogs:

- In NGFW policy-based mode, there are added tool tips under NAT columns/fields to indicate that NAT must be configured via Central SNAT Map. Additionally, links to redirect to Central SNAT list were added.
- Default `ssl-ssh-profile` is shown in the policy list and dialog for any policies doing NGFW (`application, application-categories, url-categories`) or UTM (`av-profile etc.) inspection.
  - Default `ssl-ssh-profile` is disabled from editing in policy list dialog

Central SNAT Policy list and dialogs:

- In both `profile-based` & `policy-based` `ngfw-mode`, fields for `srcintf`, `dstintf` were added to Central SNAT policies entries.
- In `policy-based` mode only, a toggle-switch for ***NAT Action*** was added in Central SNAT policy dialog. The action is also configurable from the ***Action*** column in Central SNAT policy list.

SSL/SSH Inspection list:

- In policy-based mode only, the navigation bar link to ***SSL/SSH Inspection*** redirects to the profiles list
- In policy-based mode only, the ***SSL/SSH Inspection*** list table indicates which profile is the current VDOM default. Additionally, options are provided in the list menu and context menu to change the current VDOM default.

Managed FortiSwitch

New managed FortiSwitch features added to FortiOS 5.6 if the FortiSwitch is running FortiSwitch OS 3.5.4,

Aggregating FortiSwitches into groups (397950)

In larger networks, the number of switches can be large. Different models and device purposes might exist. Furthermore, the topology might have "built-in" redundancy. Use the following command to create a FortiSwitch group allowing you to perform an operation on the entire group instead of one switch at a time.

```
config switch-controller switch-group
   edit <name>
      set description <string>
      set members <..> <..>
      end
   end
```

Pre-authentication and Replacements of FortiSwitches (298533)

FortiSwitch configuration templates allow you to replace a FortiSwitch and have the configuration of the original FortSwitch installed on the replacement.

Use the `execute replace-device fortiswitch <sn-old> <sn-new>` to transfer the configuration for the FortiSwitch with serial number `<sn-old>` to the replacement FortiSwitch with serial number `<sn-new>`.

LLDP MED on Managed FortiSwitches (372288)

FortiOS 5.6 supports configuring Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP MED) for managed FortiSwitches. Additionally, you can use FortiGate CLI commands display the information collected by LLDP on the FortiSwitch.

You can use the following command to add Media Endpoint Discovery (MED) features to an LLDP profile.

```
config switch-controller lldp-profile
   edit <lldp-profle>
        config med-network-policy
           edit guest-voice
              set status {disable | enable}
           next
           edit guest-voice-signaling
              set status {disable | enable}
           next
           edit guest-voice-signaling
              set status {disable | enable}
           next
           edit softphone-voice
              set status {disable | enable}
           next
           edit streaming-video
              set status {disable | enable}
           next
           edit video-conferencing
```

```
            set status {disable | enable}
         next
         edit video-signaling
            set status {disable | enable}
         next
         edit voice
            set status {disable | enable}
         next
         edit voice-signaling
            set status {disable | enable}
         end
      config custom-tlvs
         edit <name>
            set oui <identifier>
            set subtype <subtype>
            set information-string <string>
         end
   end
```

Enhanced 802.1x including FortiSwitch port security policy framework (389102)

New FortiSwitch port security features include:

- Dynamic VLAN Assignment
- “guest” and “auth-fail” VLAN
- Mac Address Bypass (MAB)
- Multiple host support on single physical port

Global Settings Applied across the Network

```
config switch-controller 802.1x-settings
   set reauth-period < int >
   set max-reauth-attempt < int >
   set link-down-auth < *set-unauth | no-action >
end
```

Local Switch Overrides

```
config switch-controller managed-switch
   edit < switch >
      config 802.1x-settings
         set local-override {disable | enable}
         set reauth-period <int>
         set max-reauth-attempt <int>
         set link-down-auth {set-unauth | no-action}
      end
   next
end
```

Policy Definitions (802.1x, and captive-portal)

```
config switch-controller security-policy 802.1x
   edit 8021X-policy-default
      set user-group <user.group>
```

```
      set mac-auth-bypas {disable | enable}
      set guest-vlan {disable | enable}
      set guest-vlanid <vlan-id>
      set guest-auth-delay <int>
      set auth-fail-vlan  {disable | enable}
      set auth-fail-vlanid <vlan-id>
      radius-timeout-overwrite {disable | enable}
   end
end


config switch-controller security-policy captive-portal
   edit captive-portal-default
      set vlan <vlan-id>
      config users
         edit 1
            set user-group <usergroup>
            set vlanid <vlan-id>
         next
      end
   end
end
```

Port Settings

```
config switch-controller managed-switch
   edit <managed-switch>
      config ports
         edit <port>
            set port-security-policy {802.1x-policy | captive-portal-policy}
         next
      end
   next
end
```

Firmware upgrade management and compatible version information (385171)

You can view the current firmware version of a FortiSwitch and upgrade the FortiSwitch to a new firmware version by going to **WiFi & Switch Controller > Managed FortiSwitch** and editing one of the FortiSwitches. Under **Firmware** you can see the current firmware version and select **Update** to update it.

Changed Managed-Switch Display Format for 'dynamic-capability' (387239)

FortiOS 5.6.0 displays capability flags as strings such as: dynamic-capability, igmp-snooping, dhcp-snooping, and so on. For example:

```
config switch-controller managed-switch
edit S124DP3X15000315
get
switch-id : S124DP3X15000315
name :
description :
fsw-wan1-peer : port9
```

```
fsw-wan1-admin : enable
fsw-wan2-peer :
fsw-wan2-admin : discovered
directly-connected : 0
connected : 1
version : 1
pre-provisioned : 0
dynamic-capability : igmp-snooping,dhcp-snooping
switch-device-tag :
dynamically-discovered: 1
```

Connecting to a managed switch CLI from the FortiGate GUI (378119)

To connect to a FortiSwitch CLI, go to **WiFi & Switch Controller > Managed FortiSwitch**, right click on the FortiSwitch to connect to and select **Connect to CLI**. You can also open the FortiGate CLI console and use the `execute telnet <ip>` command, where `<ip>` is the management IP address of the FortiSwitch.

Firmware upgrade of stacked or tiered switches (355050)

From your FortiGate CLI, you can upgrade the firmware of all of the managed FortiSwitches of the same model using a single `execute` command. The command includes the name of a firmware image file and all of the managed FortiSwitches compatible with that firmware image file are upgraded. For example:

```
execute switch-controller stage-swtp-image ALL <firmware-image-file>
```

You can also use the following new command to restart all of the managed FortiSwitches after a 2 minute delay.

```
execute switch-controller restart-swtp-delayed ALL
```

More information displayed by the execute switch-controller get-conn-status command (388751)

The `get-conn-status` command now displays more information for each managed switch including the ID of each switch, the version of the firmware running on the switch, the status of the switch, the IP address for managing the switch, and its join time.

```
execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-port3
SWITCH-ID        VERSION  STATUS          ADDRESS     JOIN-TIME NAME
FS108D3W16001177 v3.4     Authorized/Down 169.254.1.2 N/A       My-Switch
```

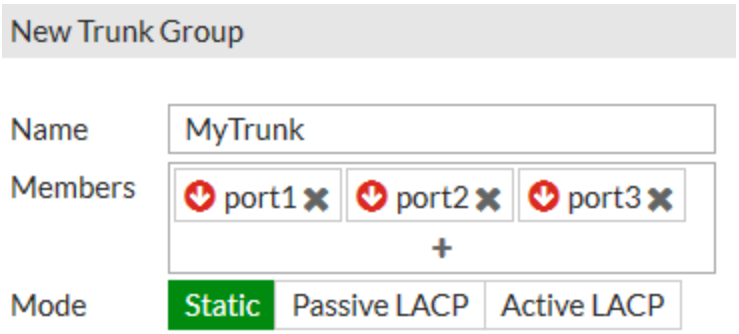
User-port Link Aggregation Groups available on the GUI (378470)

The GUI now supports the ability to configure user port LAGs on managed FortiSwitches.

To create a Link Aggregation Group for FortiSwitch user ports:

1. Go to **WiFi & Switch Controller > FortiSwitch Ports**.
2. Click **Create New > Trunk**.
3. In the New Trunk Group page enter a **Name** for the trunk group.
4. Select two or more physical ports to add to the trunk group.

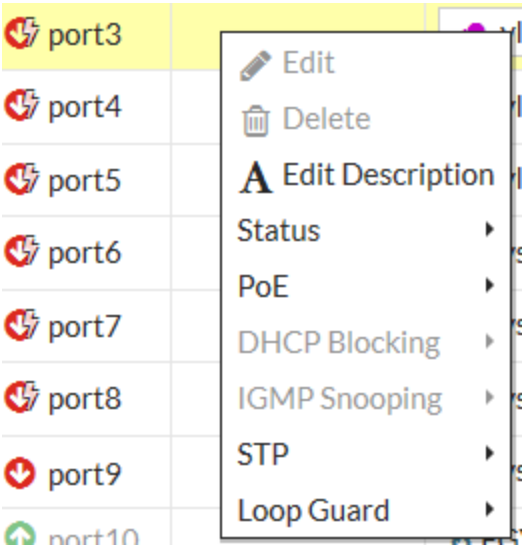
5. Select the **Mode**: Static, Passive LACP, or Active LACP.
6. Click OK.



DHCP blocking, STP and Loop Guard on Managed FortiSwitch ports on the GUI (375860)

The managed FortiSwitch GUI now supports the ability to enable/disable DHCP blocking, STP and Loopguard for FortiSwitch user ports.

Go to **WiFi & Switch Controller > FortiSwitch Ports**. For any port you can select DHCP Blocking, STP, or Loop Guard. STP is enabled on all ports by default. Loop guard is disabled by default on all ports.



New Switch Profiles (387398)

Switch profiles allow specific settings to be applied to all authorized FortiSwitches. The default switch profile is automatically bound to every switch discovered by the FortiGate. You can create additional profiles as needed.

Within a switch profile, you can control the behavior of the FortiSwitch's admin account.You can add a password to a profile or create a new profile and bind that profile to any switch. The password provided in the profile is configured on the FortiSwitch to the default admin administrator account.

Miscellanous configuration option changes

- On a switch port, the default value of `dhcp-snooping` (also called DHCP-blocking) is changed from `trusted` in FortiOS 5.4 to `untrusted` in FortiOS 5.6.
- On a switch port, the default value of STP `edge-port` is changed from `disabled` in FortiOS 5.4 to `enabled` in FortiOS 5.6.0.
- Default value of `fortilink-split-port` is changed from `disable` in FortiOS 5.4.1/5.4.2 to `enable` in FortiOS 5.4.3 onward. This command applies to FortiGate aggregate interfaces.

```
config system interface
   edit <name of the FortiLink interface>
      set fortilink-split-interface enable
   end
```

FortiView

New FortiView features added to FortiOS 5.6.

Added Vulnerability score topology view (303786)

In **Physical Topology** and **Logical Topology** pages, there are two new views added: ***Vulnerability***, and ***Threat***. Drill-downs in these menus will now include Vulnerability/Threat information. In Vulnerability view, device bubbles are colored based on maximum vulnerability level, and bubble size is the vulnerability score. In Threat view, device bubbles are colored based on maximum threat level, and bubble size is the threat score.

FortiView VPN tunnel map feature (382767)

The FortiView VPN page now displays VPN tunnel connections between devices, and offers more information about tunnels and devices on drill-down.

Updated FortiView CSF topology pages (384188)

The FortiView **Physical Topology** and **Logical Topology** pages have been updated in 5.6.0 to reorganize and clarify larger deployments with servers and multi-directional traffic.

Historical FortiView includes FortiAnalyzer (387423)

Data from associated FortiAnalyzer devices can now be selected as a log display option for Historical FortiView.

FortiView menu reorganization (399713)

The order of FortiView pages has been reorganized in 5.6.0 based on the source interface of data being displayed:

- Topology
- Traffic from LAN/DMZ

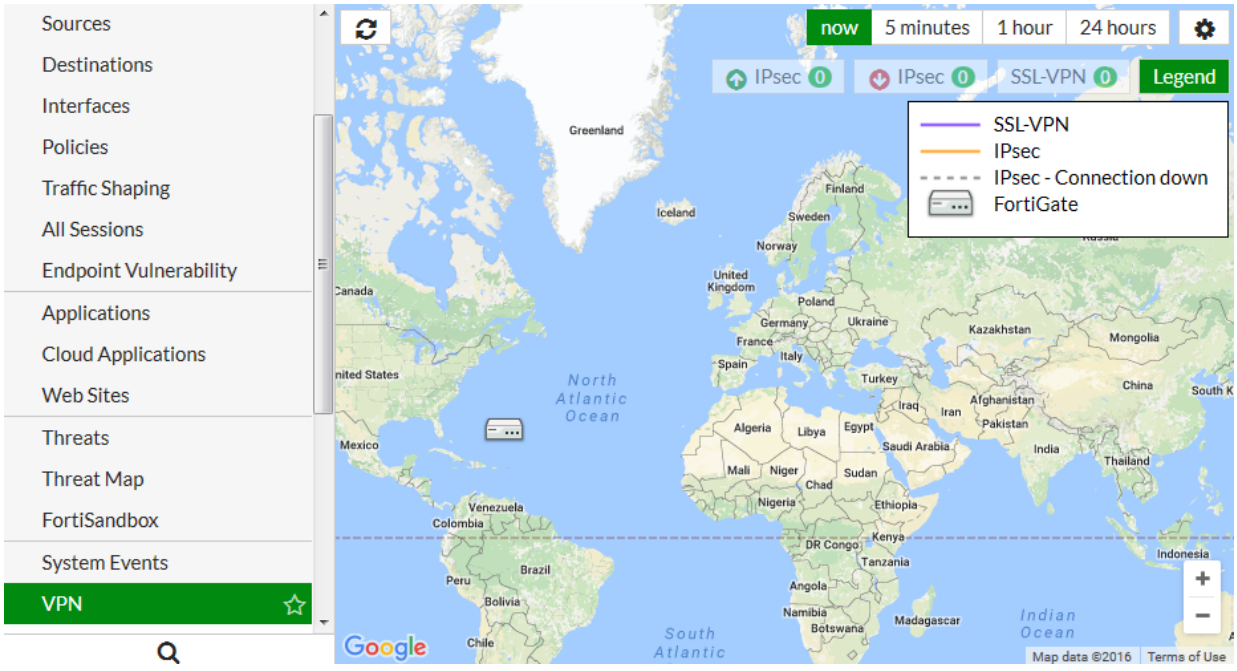
- Traffic from WAN
- All Segments

Data Exchange with FortiAnalyzer (393891)

Rather than sending all CSF information via log messages, FortiGate and FortiAnalyzer will now directly pass CSF information (tree, interface roles, user devices, HA members), if the FAZ responds to notices that are sent when the data has changed.

Google Maps Integration

FortiView now uses Google Maps to display location-related information. In this release the first view to use Google maps this component is the FortView VPN page. All current VPNs can be viewed on a fully scalable Google world map.



FortiView usability and organization updates (306247)

Several organization changes have been made to make the FortiView menu order less cluttered, and more intuitive.

- **WiFi Client** Monitor is now in FortiView, but is hidden when there is no managed FortiAP or WiFi Radio.
- **Country** view has been merged into **Destinations** view.
- **Failed Authentication** and **Admin Login** views have been merged into **System Events** view.

FortiGate VM

New FortiGate VM features added to FortiOS 5.6.

FGT-VM VCPUs (308297)

Fortinet has now launched licensing for FortiGate VMs that support larger than 8 vCPUs. The new models/licenses include:

- Support for up to 16 vCPU - FortiGate-VM16
- Support for up to 32 vCPU - FortiGate-VM32
- Support for unlimited vCPU - FortiGate-VMUL

Each of these models should be able to support up to 500 VDOMs.

Improvements to License page (382128)

The page has been rewritten with some minor improvements such as:

- An indicator to show when a VM is waiting for authentication or starting up
- Shows VM status when license is valid
- Shows CLI console window when VM is waiting too long for remote registration of server

Citrix XenServer tools support for XenServer VMs (387984)

This support allows users, with Citrix XenServer tools to read performance statistics from XenServer clients and do Xenmotion with servers in the same cluster

Since FortiGates don't support hardware hotplugging, the ability to do network interface of disk changes is not supported at this time.

There are no changes to the GUI, but there are some changes to the CLI.

A setting has been edited to control the debug level of the XenServer tools daemon

```
diag debug application xstoolsd <integer>
```

Integer = Debug level

An additional update has been added to set the update frequency for XenServer tools

```
config system global
   set xstools-update-frequency Xenserver <integer>
   end
```

Enter an integer value from `30` to `300` (default = 60).

FOS VM supports more interfaces (393068)

The number of virtual interfaces that the VM version of FortiOS supports has been raised from 3 to 10.

NSX security group importing (403975)

A feature has been added to allow the importation of security group information from VMware's NSX firewall.

CLI Changes:

nsx group list

This is used to list NSX security Groups

Syntax:

```
execute nsx group list <name of the filter>
```

nsx group import

This is used to import NSX security groups.

Syntax:

```
execute nsx group import <vdom> <name of the filter>
```

nsx group delete

This is used to delete NSX security Groups

Syntax:

```
execute nsx group delete <vdom> <name of the filter>
```

nsx.setting.update-period

This is used to set the update period for the NSX security group

Syntax:

```
config.nsx.setting.update-period <0 - 3600 in seconds>
```

`0` means disabled

Default value: `0`

Non-vdom VM models FGVM1V/FGVM2V/FGVM4V (405549)

New models of the FortiGate-VM have been introduced. These match up with the existing FortiGate-VM models of FG-VM01, FG-VM02 and FG-VM04. The difference being that the new models don't support VDOMs.

Original FortiGate-VM	New FortiGate-VM without VDOM support
FG-VM01	FG-VM01v
FG-VM02	FG-VM02v
FG-VM04	FG-VM04v

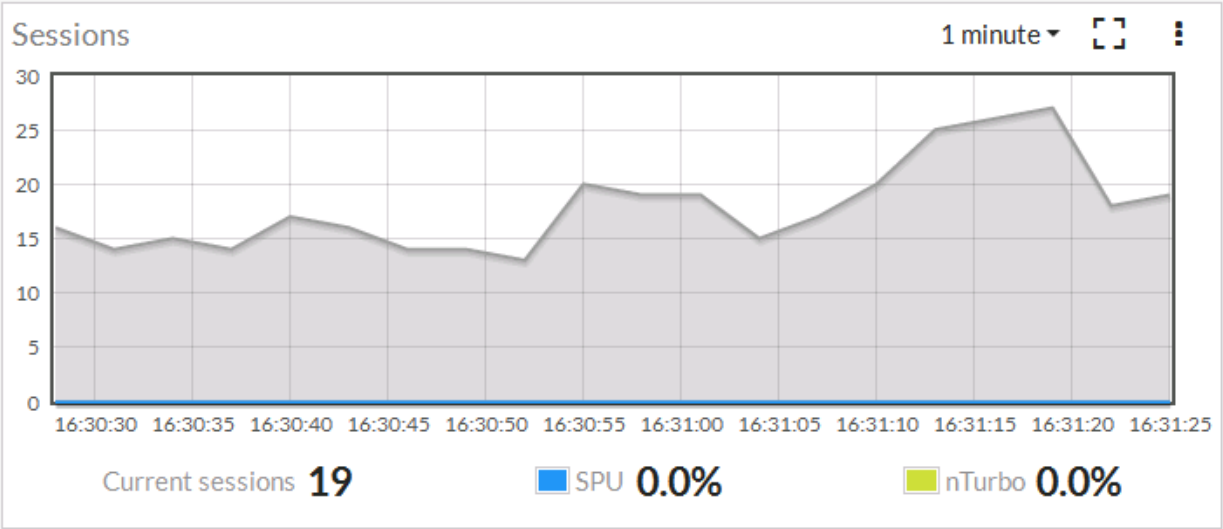
Hardware acceleration

New hardware acceleration features added to FortiOS 5.6.

Improved visibility of SPU and nTurbo hardware acceleration (389711)

All hardware acceleration hardware has been renamed Security Professing Units (SPUs). This includes NPx and CPx processors.

SPU and nTurbo data is now visible in a number of places on the GUI. For example, the Active Sessions column pop-up in the firewall policy list and the Sessions dashboard widget:



You can also add SPU filters to many FortiView pages.

NP4Lite option to disable offloading ICMP traffic in IPsec tunnels (383939)

In some cases ICMP traffic in IPsec VPN tunnels may be dropped by the NP4Lite processor due to a bug with the NP4Lite firmware. You can use the following command to avoid this problem by preventing the NP4Lite processor from offloading ICMP sessions in IPsec VPN tunnels. This command is only available on FortiGate models with NP4Lite processors, such as the FortiGate/FortiWiFi-60D.

```
config system npu
   set process-icmp-by-host {disable | enable}
end
```

The option is disabled by default an all ICMP traffic in IPsec VPN tunnels is offloaded where possible. If you are noticing that ICMP packets in IPsec VPN tunnels are being dropped you can disable this option and have all ICMP traffic processed by the CPU and not offloaded to the NP4Lite.

NP6 IPv4 invalid checksum anomaly checking (387675)

The following new options have been added to NP6 processors to check for IPv4 checksum errors in IPv4, TCP, UDP, and ICMP packets:

```
config system np6
   edit {np6_0 | np6_1| ...}
      config fp-anomaly-v4
         set ipv4-csum-err {drop | trap-to-host}
         set tcp-csum-err {drop | trap-to-host}
         set udp-csum-err {drop | trap-to-host}
         set icmp-csum-err {drop | trap-to-host}
      end
```

You can use the new options to either drop packets with checksum errors (the default) or send them to the CPU for processing. Normally you would want to drop these packets.

High Availability

New High Availability features added to FortiOS 5.6.

Multicast session failover (293751)

FGCP HA multicast session synchronization supports multicast session failover. To configure multicast session failover, use the following command to change the multicast TTL timer to a smaller value than the default. The recommended setting to support multicast session failover is 120 seconds (2 minutes). The default setting is 600 seconds (10 minutes).

```
config system ha
   set multicast-ttl 120
end
```

The multicast TTL timer controls how long to keep synchronized multicast routes on the backup unit (so they are present on the backup unit when it becomes the new primary unit after a failover). If you set the multicast TTL lower the multicast routes on the backup unit are refreshed more often so are more likely to be accurate. Reducing this time causes route synchronization to happen more often and could affect performance.

Performance improvement when shutting down or rebooting the primary unit (380279)

In previous versions of FortiOS, if you entered the `execute reboot` or `execute shutdown` command on the primary unit, a split brain configuration could develop for a few seconds while the primary unit was shutting down. This would happen because the heartbeat packets would stop being sent by the primary unit, while it was still able to forward traffic. When the heartbeat packets stop the backup unit becomes the primary unit. The result was a split brain configuration with two primary units both capable of forwarding traffic.

This wouldn't happen all the time, but when it did network traffic would be delayed until the primary unit shut down completely. To resolve this issue, in FortiOS 5.6 when you run the `execute reboot` or `execute shutdown` command on the primary unit, the primary unit first becomes the backup unit before shutting down allowing the backup unit to become the new primary unit and avoiding the split brain scenario. This behavior only happens when you manually run the `execute reboot` or `execute shutdown` command from the primary unit.

VRRP failover process change (390938)

In a FortiOS 5.6 VRRP configuration, when the master cannot reach its next hop router (vrdst) it sends packets to the configured backup router(s). These packets set the priority of the master to be lower than the backup router (s). So a backup router now becomes the new master and takes over processing traffic.

Use the `vrdst-priority` option to set the lower priority that the master sends to the backup routers. The following CLI syntax resets the master's priority to 10 if it can no longer connect to its next hop router.

```
config system interface
   edit port10
      config vrrp
         set vrip 10.31.101.200
         set priority 255
         set vrdst 10.10.10.1
         set vrdst-priority 10
```

```
    end
```

Display cluster up time and history (get system ha status command changes)(394745)

The get system HA status command now displays cluster uptime and history:

```
get system status
Version: FortiGate-5001D v5.6.0,build1413,170121 (interim)
...
Current HA mode: a-p, master
Cluster uptime: 3 days, 4 hours, 3 minutes, 46 seconds
...
```

In-band HA management Interface (401378)

You can use the following command to add a management interface to an individual cluster unit interface that is also connected to a network and processing traffic. The in-band management interface is an alternative to the reserved HA management interface feature and does not require reserving an interface just for management access.

```
config system interface
   edit port1
      set management-ip 172.20.121.155/24
   end
```

The management IP address is accessible from the network that the cluster interface is connected to. This setting is not synchronized so each cluster unit can have their own management IP addresses. You can add a management IP address to each cluster unit interface. You can use the `execute ha manage` command to connect to individual cluster units.

The `management-ip` can be on the same subnet as the interface you are adding it to but cannot be on the same subnet as other cluster unit interfaces.

Up to four dedicated HA management interfaces supported (378127)

You can now add up to four dedicated HA management interfaces. Just like all FortiGate interfaces, these management interfaces must be on a different subnet from any other FortiGate interface. You can also configure a separate default gateway for each interface.

Use the following command to add two dedicated HA management interfaces:

```
config system ha
   set ha-mgmt-status enable
      config ha-mgmt-interfaces
         edit 1
            set interface port4
            set gateway 10.10.10.1
         next
         edit 2
            set interface port5
            set gateway 4.5.6.7
         end
```

FGSP support for automatic session sync after peer reboot (365851)

New options allow you to configure your FGSP cluster to resume sessions more smoothly after a failed FortiGate rejoins the cluster. In some cases when a failed FortiGate in the cluster comes back up it may begin processing sessions before the session table has been synchronized to it from the other FortiGate in the cluster. When this happens, the FortiGate may drop packets until the session synchronization is complete.

Shutting down interfaces during session synchronization

This new feature allows you to shut some interfaces down on the failed FortiGate when it is starting up so that it will not accept packets until session synchronization is complete. Then the interfaces are brought up and traffic can flow. While the interfaces are down, the FortiGate that had not failed keeps processing traffic.

Use the following command to select the interfaces to shutdown while waiting for session synchronization to complete:

```
config system cluster-sync
   edit 1
      set down-intfs-before-sess-sync port1 port2
   end
```

Heartbeat monitoring

If the FortiGate that was running fails before session synchronization is complete, the FortiGate that is restarting would not be able to complete session synchronization and would not turn on its shutdown interfaces. To prevent this from happening FGSP now includes heartbeat monitoring. Using heartbeat monitoring the FortiGate that is waiting for session synchronization to finish can detect that the other FortiGate is down and turn on its interfaces even if session synchronization is not complete. You can use the following command to change the heartbeat interval (`hb-interval`) and lost heartbeat threshold (`hp-lost-threshold`) to change heartbeat monitoring timing.

```
config system cluster-sync
   edit 1
      set hb-interval 2
      set hb-lost-threshold 3
   end
```

Change in cluster behavior when the primary unit is restarted (380279)

When testing HA failover or restarting the primary unit for other reasons, manually rebooting or shutting down the primary unit running previous versions of FortiOS can sometimes cause a failover delay. This happens because the backup unit may become the primary unit before the primary unit is fully shut down causing a temporary split brain scenario.

To resolve this issue, when you manually restart or shut down the primary unit running FortiOS 5.6.0 before the primary unit actually shuts down it becomes the backup unit and the previous backup unit becomes the primary unit. Traffic is then failed over to the new primary unit before the former primary unit shuts down or reboots.

This chapter describes new high availability features added to FortiOS 5.6.

IPsec VPN

New IPsec VPN features added to FortiOS 5.6.

Improvement to stats crypto command output (403995)

The CLI command `get vpn ipsec stats crypto` now has a better format for the information it shows in differentiating between NP6 lite and SOC3 (CP). To further avoid confusion, all engine's encryption (encrypted/decrypted) and integrity (generated/validated) information is shown under the same heading, not separate headings.

Improved certificate key size control commands (397883)

Proxy will choose the same SSL key size as the HTTPS server. If the key size from the server is 512, the proxy will choose 1024. If the key size is bigger than 1024, the proxy will choose 2048.

As a result, the `firewall ssl-ssh-profile` commands `certname-rsa`, `certname-dsa`, and `certname-ecdsa` have been replaced with more specific key size control commands under `vpn certificate setting`.

CLI syntax

```
config vpn certificate setting
   set certname-rsa1024 <name>
   set certname-rsa2048 <name>
   set certname-dsa1024 <name>
   set certname-dsa2048 <name>
   set certname-ecdsa256 <name>
   set certname-ecdsa384 <name>
end
```

Support bit-based keys in IKE (397712)

As per FIPS-CC required standards, as well as RFC 4306, IKE supports pre-shared secrets to be entered as both ASCII string values and as hexadecimal encoded values. This feature parses hex encoded input (indicated by the leading characters **0x**) and converts the input into binary data for storage.

With this change, the `psksecret` and `psksecret-remote` entries under the IPsec VPN CLI command `config vpn ipsec-phase1-interface` have been amended to differentiate user input as either ASCII string or hex encoded values.

IKEv2 asymmetric authentication (393073)

Support added for IKEv2 asymmetric authentication, allowing both sides of an authentication exchange to use different authentication methods, for example the initiator may be using a shared key, while the responder may have a public signature key and certificate.

A new command, `authmethod-remote`, has been added to `config vpn ipsec phase1-interface`.

For more detailed information on authentication of the IKE SA, see RFC 5996 - Internet Key Exchange Protocol Version 2 (IKEv2).

Allow mode-cfg with childless IKEv2 (391567)

An issue that prevented `childless-ike` from being enabled at the same time as `mode-cfg` has been resolved. Both options can now be enabled at once under `config vpn ipsec phase1-interface`.

IKEv2 Digital Signature Authentication support (389001)

FortiOS supports the use of Digital Signature authentication, which changes the format of the Authentication Data payload in order to support different signature methods.

Instead of just containing a raw signature value calculated as defined in the original IKE RFCs, the Auth Data now includes an ASN.1 formatted object that provides details on how the signature was calculated, such as the signature type, hash algorithm, and signature padding method.

For more detailed information on IKEv2 Digital Signature authentication, see RFC 7427 - Signature Authentication in the Internet Key Exchange Version 2 (IKEv2).

Passive static IPsec VPN (387913)

New commands have been added to `config vpn ipsec phase1-interface` to prevent initiating VPN connection. Static IPsec VPNs can be configured in tunnel mode, without initiating tunnel negotiation or rekey.

To allow a finer configuration of the tunnel, the rekey option is removed from `config system global` and added to `config vpn ipsec phase1-interface`.

CLI syntax

```
config vpn ipsec phase1-interface
   edit <example>
      set rekey {enable | disable}
      set passive-mode {enable | disable}
      set passive-tunnel-interface {enable | disable}
end
```

Phase 2 wizard simplified (387725)

Previously, for a site-to-site VPN, phase 2 selectors had their static routes created in the IPsec VPN wizard by adding IP addresses in string format. Now, since addresses and address groups are already created for these addresses, the address group can be used in the route directly. This means that the route can be modified simply by modifying the address/groups that were created when the VPN was initially created.

With this change, the VPN wizard will create less objects internally, and reduce complexity.

In addition, a blackhole route route will be created by default with a higher distance-weight set than the default route. This is to prevent traffic from flowing out of another route if the VPN interface goes down. In these instances, the traffic will instead be silently discarded.

Unique IKE ID enforcement (383296)

All IPsec VPN peers now connect with unique IKE identifiers. To implement this, a new `phase1` CLI command has been added (`enforce-unique-id`) which, when enabled, requires all IPsec VPN clients to use a unique identifier when connecting.

CLI syntax

```
config vpn ipsec phase1
   edit <name>
      set enforce-unique-id {keep-new | keep-old | disable} Default is disable.
   next
end
```

Use `keep-new` to replace the old connection if an ID collision is detected on the gateway.
Use `keep-old` to reject the new connection if an ID collision is detected.

FortiView VPN tunnel map feature (382767)

A geospatial map has been added to FortiView to help visualize IPsec and SSL VPN connections to a FortiGate using Google Maps. Adds geographical-IP API service for resolving spatial locations from IP addresses.

This feature can be found under **FortiView > VPN**.

Childless IKEv2 initiation (381650)

As documented in RFC 6023, when both sides support the feature, no child IPsec SA is brought up during the initial AUTH of the IKEv2 negotiation. Support for this mode is not actually negotiated, but the responder indicates support for it by including a CHILDLESS_IKEV2_SUPPORTED Notify in the initial SA_INIT reply. The initiator is then free to send its AUTH without any SA or TS payloads if it also supports this extension.

CLI syntax

```
config vpn ipsec phase1-interface
   edit ike
      set ike-version 2
      set childless-ike enable
   next
end
```

Due to the way configuration payloads (IKEV2_PAYLOAD_CONFIG) are handled in the current code base, mode-cfg and childless-ike aren't allowed to be enabled at the same time. Processing config payloads for mode-cfg requires a child ph2handle to be created, but with childless-ike we completely avoid creating the child ph2 in the first place which makes the two features incompatible. It may be possible to support both in the future, but a deeper rework of the config payload handling is required.

Allow peertype dialup for IKEv2 pre-shared key dynamic phase1 (378714)

Restored `peertype dialup` that was removed in a previous build (when IKEv2 PSK gateway re-validation was not yet supported).

If `peertype` is `dialup`, IKEv2 AUTH verify uses user password in the user group "usrgrp" of phase1. The "psksecret" in phase1 is ignored.

CLI syntax

```
config vpn ipsec phase1-interface
   edit "name"
      set type dynamic
      set interface "wan1"
      set ike-version 2
      set peertype dialup
      set usrgrp "local-group"
   next
end
```

IPsec default phase1/phase1-interface peertype changed from 'any' to 'peer' (376340)

Previously, when `authmethod` was changed to `signature`, `peertype` automatically changed to `peer` and required a peer to be set. This change was done to try to provide a more secure initial configuration, while allowing the admin to set `peertype` back to `any` if that's what they really wanted. The default value was kept at `any` in the CLI. However, this caused problems with copy/pasting configurations and with FMG because if `peertype any` wasn't explicitly provided, the CLI was switched to `peertype peer`.

This patch changes the default peertype to `peer` now; peertype `any` is considered non-default and will be printed out on any config listing. Upgrade code has been written to ensure that any older build that was implicitly using `set peertype any` has this setting preserved.

IPsec GUI bug fixes (374326)

Accept type "Any peer ID" is available when creating IPsec tunnel with authmethod, pre-shared key, ikev1 main mode/aggressive mode, and ikev2.

Support for IKEv2 Message Fragmentation (371241)

Added support for IKEv2 Message Fragmentation, as described in RFC 7383.

Previously, when sending and IKE packets with IKEv1, the whole packet is sent once, and it is only fragmented if there is a retransmission. With IKEv2, because RFC 7383 requires each fragment to be individually encrypted and authenticated, we would have to keep a copy of the unencrypted payloads around for each outgoing packet, in case the original single packet was never answered and we wanted to retry with fragments. So with this implementation, if the IKE payloads are greater than a configured threshold, the IKE packets are preemptively fragmented and encrypted.

CLI syntax

```
config vpn ipsec phase1-interface
   edit ike
```

```
        set ike-version 2
        set fragmentation [enable|disable]
        set fragmentation-mtu [500-16000]
    next
end
```

IPsec monitoring pages now based on phase 1 proposals not phase 2 (304246)

The IPsec monitor, found under **Monitor > IPsec Monitor**, was in some instances showing random uptimes even if the tunnel was in fact down.

Tunnels are considered as "up" if at least one phase 2 selector is active. To avoid confusion, when a tunnel is down, **IPsec Monitor** will keep the **Phase 2 Selectors** column, but hide it by default and be replaced with **Phase 1** status column.

IPv6

New IPv6 features added to FortiOS 5.6.

FortiGate can reply to an anycast probe from the interface's unicast address (308872)

A new setting has been added within the CLI that can enable the FortiGate to reply to an anycast probe from the FortiGate's unicast IP address.

```
config system global
   set ipv6-allow-anycast-probe [enable|disable]
   end
```

Enable: Enable probing of IPv6 address space through Anycast, by responding from the unicast IP address

Disable: Disable probing of IPv6 address space through Anycast

Secure Neighbor Discovery (355946)

Additional settings have been added to the configuration for interfaces with IPv6 so that they comply more closely to the parameters of RFC 3971

The context of the new settings is

```
config system interface
   edit <interface>
   config ipv6
```

The new options with IPv6 are:

ndmode

Neighbor discovery mode

```
set ndmode [basic | SEND]
```

Basic: Does not support SEND.

SEND-compatible: Supports SEND.

nd-cert

Neighbor discovery certificate

```
set nd-cert <string of Name of certificate to be used>
```

Example string: `"Fortinet_Factory local"`

n-security-level

Neighbor discovery security level

```
set nd-security-level <integer>
```

- Integer values from 0 - 7
- 0 = least secure
- 7 = most secure
- default = 0

nd-timestamp-delta -

Neighbor discovery timestamp delta value

```
set nd-timestamp-delta <integer of time in seconds>
```

- Range: 1 - 3600 sec
- default = 300

nd-timestamp-fuzz

Neighbor discovery timestamp fuzz factor

```
set nd-timestamp-fuzz <integer of time in seconds>
```

- Range: 1 - 60 sec
- default = 1

Additional related technical information

Kerenl

- Redirects ICMPv6 packets to user space if they require SEND options verification or build.

Radvd

- Verifies NS/RS SEND options including CGA, RSA, Timestamp, NONCE, etc. Daemon also creates neighbor cache for future timestamp checking, any entry gets flushed in 4 hours.
- Helps kernel build NA/RA SEND options including CGA, RSA, Timestamp, NONCE, etc. CGA parameters are kept in cache for each interface. CGA modifier is kept in CMDB.

Diagnose command for radvd

```
diag test application radvd
```

- Shows statistics
- Toggles message dump

Add multicast-PMTU to allow FGT to send ICMPv6 Too Big Message (373396)

New multicast-PMTU feature added to better comply with RFC 4443.

Normally, a “Packet Too Big” icmp6 message is sent by a routing device in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link. For security reasons, these message may be disabled because attackers can use the information about a victim's ip address as the source address to do IP address spoofing.

In FortiOS's implementation of this function, a setting in the CLI, has been added to make this behavior optional on the FortiGate.

The syntax for the option is:

```
config router multicast6
   set multicast-PMTU [enable|disable]
   end
```

Logging and Reporting

New logging and reporting features added to FortiOS 5.6.

Client and server certificates included in Application control log messages (406203)

When SSL/TLS traffic triggers an application control signature, the application control log messages now include information about the signatures used by the session. This includes the client certificate issuer, the name in the server certificate, and the server certificate issuer.

DNS Logging (401757)

FortiOS logging now includes the Detailed DNS log message type. DNS events were previously recorded as event logs. In FortiOS 5.6 DNS log messages are a new category that also includes more DNS log messages to provide additional detail about DNS activity through the FortiGate. You can enable DNS logging from the CLI using the following command (shown in this example for memory logging):

```
config log memory filter
   set dns enable
end
```

DNS log messages include details of each DNS query and response. DNS log messages are recorded for all DNS traffic though the FortiGate and originated by the FortiGate.

The detailed DNS logs can be used for low-impact security investigation. Most network activity involves DNS activity of some kinds. Analyzing DNS logs can provide a lot of details about the activity on your network without using flow or proxy-based resource intensive techniques.

Added Policy Comment logging option (387865)

As an alternative to custom log fields, the functionality has been added to log a policy's comment field in all traffic log files that use that policy, in order to sort/isolate logs effectively with larger deployments and VDOMs. The feature is disabled by default.

```
config log setting
   set log policy comment [enable/disable]
```

FortiAnalyzer encryption option name change (399191)

For clarity, and because the default options for `config log fortianalyzer setting` have now changed, the option `default` has now been changed to `high-medium` in the following CLI commands:

```
config log fortianalyzer setting
   set enc-algorithm [high/high-medium/low]
config log fortinalyzer override-setting
   set enc-algorithm [high/high-medium/low]
config log fortiguard setting
   set enc-algorithm [high/high-medium/low]
config log fortiguard override-setting
   set enc-algorithm [high/high-medium/low]
```

Networking

New networking features added to FortiOS 5.6.

New command to get transceiver signal strength (205138)

On most FortiGate models with SFP/SFP+ interfaces you can use the following command to display information about the status of the transceivers installed in the SFP/SFP+ interfaces of the FortiGate.

The command output lists all of SFP/SFP+ interfaces and if they include a transceiver the output displays information about it. The command output also includes details about transceiver operation that can be used to diagnose transmission problems.

```
get system interface transceiver
...
Interface port14 - Transceiver is not detected.
Interface port15 - SFP/SFP+
  Vendor Name  :            FIBERXON INC.
  Part No.     :            FTM-8012C-SLG
  Serial No.   :            101680071708917
Interface port16 - SFP/SFP+
  Vendor Name  :            FINISAR CORP.
  Part No.     :            FCLF-8521-3
  Serial No.   :            PS62ENQ

                                        Optical      Optical      Optical
SFP/SFP+     Temperature  Voltage       Tx Bias      Tx Power     Rx Power
Interface    (Celsius)    (Volts)       (mA)         (dBm)        (dBm)
-----------  -----------  ------------  -----------  -----------  -----------
port15        N/A          N/A           N/A          N/A          N/A
port16        N/A          N/A           N/A          N/A          N/A
  ++ : high alarm, + : high warning, - : low warning, -- : low alarm, ? : suspect.
```

New BGP local-AS support (307530)

Use the following command to configure BGP local-AS support:

```
config router bgp
   config neighbor
      edit "neighbor"
         ...
         set local-as 300
         set local-as-no-prepend disable|enable
         set local-as-replace-as disable|enable
      end
```

Enable `local-as-no-prepend` if you do not want to prepend local-as to incoming updates.

Enable `local-as-replace-as` to replace a real AS with local AS in outgoing updates.

Interface setting removed from SNMP community (310665)

The SNMP GUI has been cleaned up by removing the ***Interface*** setting.

RPF checks can be removed from the state evaluation process (311005)

You can remove stateful firewall RFP state checks without fully enabling asymmetric routing. State checks can be disabled on specific interfaces. The following command shows how to disable state checks for traffic received by the wan1 interface.

Disabling state checks makes a FortiGate unit less secure and should only be done with caution.

```
config system interface
   edit wan1
      set src-check disable
   end
```

BGP graceful-restart-end-on-timer, stale-route, and linkdown-failover options (374140)

If `graceful-end-on-timer` is enabled, the BGP graceful restart process will be stopped upon expiration of the restart timer only.

If `linkdown-failover` is enabled for a BGP neighbor, the neighbor will be down when the outgoing interface is down.

If `stale-route` is enabled for a BGP neighbor, the route learned from the neighbor will be kept for the `graceful-stalepath-time` after the neighbor is down due to hold timer expiration or TCP connection failure.

```
config router bgp
   set graceful-end-on-timer disable|enable
      config neighbor
            edit 192.168.1.1
            set linkdown-failover disable|enable
            set stale-route disable|enable
```

`graceful-end-on-timer` stops BGP graceful restart process on timer only.

`linkdown-failover` and `stale-route` are options to bring down BGP neighbors upon link down and to keep routes for a period after the neighbor is down.

FQDNs can be destination addresses in static routes (376200)

FQDN firewall addresses can now be used as destination addresses in a static route.

From the GUI, to add a FQDN firewall address (or any other supported type of firewall address) to a static route in the firewall address configuration you must enable the **Static Route Configuration** option. Then when configuring the static route set **Destination** to **Named Address**.

From the CLI, first configure the firewall FQDN address:

```
config firewall address
   edit 'Fortinet-Documentation-Website'
      set type fqdn
      set fqdn docs.fortinet.com
      set allow-routing enable
   end
```

Then add the FQDN address to a static route.

```
config router static
   edit 0
      set dstaddr Fortinet-Documentation-Website
      ...
   end
```

Priority for Blackhole routes (378232)

You can now add a priority to a blackhole route to change its position relative to kernel routes in the routing table. Use the following command to add a blackhole route with a priority:

```
config router static
   edit 23
      set blackhole enable
      set priority 200
   end
```

New DDNS refresh interval (383994)

A new DDNS option has been added to configure the FortiGate to refresh DDNS IP addresses by periodically checking the configured DDNS server.

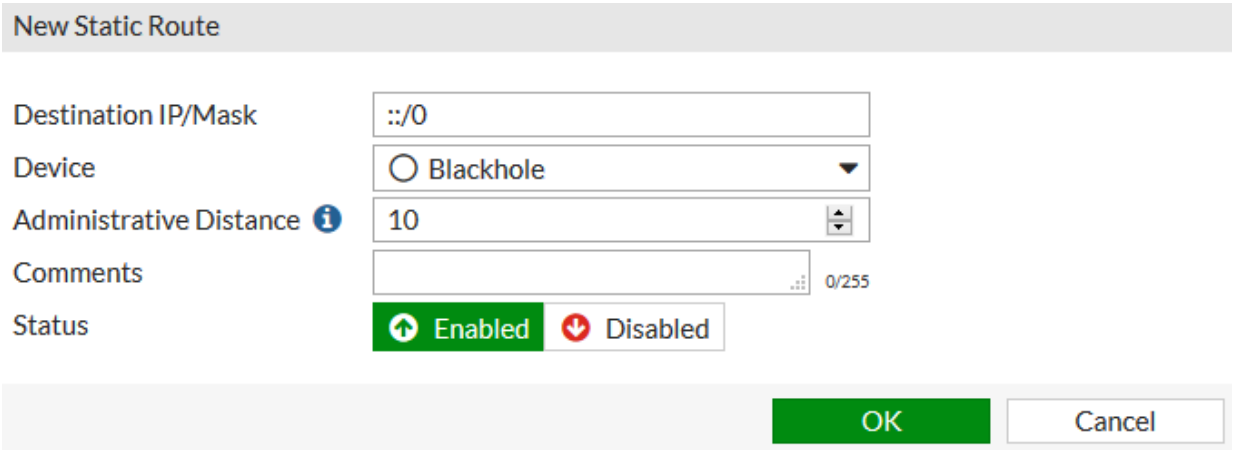
```
config system ddns
   edit 1
      set ddns-server FortiGuardDDNS
      set use-public-ip enable
      set update-interval seconds
   end
```

The default `update-interval` is 300 seconds and the range is 60 to 2592000 seconds.

Support IPv6 blackhole routes on GUI (388599)

IPv6 blackhole routes are now supported from GUI, go to **Network > Static Routes** and select **Create New > IPv6 Route**.

Choose **Blackhole** for **Device** field.



SSL-VPN can use a WAN link load balancing interface (396236)

Virtual-wan-link interface can now be set as a destination interface in SSLVPN policy.

Also SSL-VPN interface can now be set as a source interface for WAN LLB.

DDNS support for noip.com (399126)

Noip.com, and provider for Dynamic DNS has been added as a supported option for a `ddns-server`.

CLI

```
config system ddns
   edit <ddns_ip>
      set ddns-server
          [dyndns.org|dyns.net|ods.org|tzo.com|vavic.com|dipdns.net|now.net.cn||dhs.org|ea
          sydns.com|genericDDNS|FortiGuardDDNS|noip.com]
```

IPv6 Router Advertisement options for DNS (399406)

This feature is based on RFC 6106 and it adds the ability to obtain DNS search list options from upstream DHCPv6 servers and the ability to send them out through either Router Advertisement or FortiGate's DHCP server.

Configuration example:

To get the information from the upstream ISP server:

```
config system interface
   edit wan1
      config ipv6
         set dhcp6-prefix-delegation enable
      next
   next
end
```

To use Routing Advertisement to send the DNS search list:

```
config system interface
   edit port 1
      config IPv6
         set ip6-address 2001:10::/64
         set ip6-mode static
         set ip6-send-adv enable
         config ip6-delegated-prefix-list
         edit 1
            set upstream-interface WAN
            set subnet 0:0:0:11::/64
            set autonomous-flag enable
            set onlink-flag enable
         next
      next
   end
end
```

To use DHCPv6 server to send DNS search list:

```
config system dhcp6 server
   edit 1
      set interface port2
      set upstream-interface WAN
      set ip-mode delegated
      set dns-service delegated
      set dns-search-list delegated // this is a new command
      set subnet 0:0:0:12::/64
   next
end
```

WAN LLB to SD-WAN on GUI (403102)

To be more consistent with current terminology, the term ***WAN LLB*** has been changed in the GUI to the more recognizable ***SD-WAN***.

RFCs supported by FortiOS 5.6

The following RFCs are now supported by FortiOS 5.6 or the support for these RFCs has been enhanced in FortiOS 5.6:

RFC 7427 Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) (389001)

RFC 7348 Virtual eXtensible Local Area Network (VXLAN) or VTEP (289354)

RFC 5996 (section 2.15) IKEv2 asymmetric authentication (393073)

RFC 6106 IPv6 Router Advertisement Options for DNS (399406)

RFC 7383 Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation (371241)

RFC 3971 IPv6 SEcure Neighbor Discovery (SEND) (355946)

RFC 6023 Childless IKEv2 Initiation (381650)

Security Profiles

New security profile features added to FortiOS 5.6.

New FortiGuard Web Filter categories (407574)

New categories added to FortiGuard Web Filter sub-categories:

- Under Security Risk:
  - Newly Observed Domain (5.90)
  - Newly Registered Domain (5.91)
- Under General Interest - Business
  - Charitable Organizations (7.92)
  - Remote Access (7.93)
  - Web Analytics (7.94)
  - Online Meeting (7.95)

Newly observed domain (NOD) applies to URLs whose domain name is not rated and were observed for the first time in the past 30 minutes.

Newly registered domain (NRD) applies to URLs whose domain name was registered in the previous 10 days.

Overall improvement to SSL inspection performance (405224)

The enabling / disabling of proxy cipher / kxp hardware acceleration in CP8/CP9 required restarting of the WAD daemon for the change to take effect; this bug has been repaired.

New CLI commands

The FortiGate will use the `ssl-queue-threshold` command to determine the maximum queue size of the CP SSL queue. In other words, if the SSL encryption/decryption task queue size is larger than the threshold, the FortiGate will switch to use CPU rather than CP. If less, it will employ CP.

```
config firewall ssl setting
   set ssl-queue-threshold <integer>
end
```

The integer represents the maximum length of the CP SSL queue. Once the queue is full, the proxy switches cipher functions to the main CPU. The range is 0 - 512 and the default is 32.

FortiClient Endpoint license updates (401721)

FortiClient endpoint licenses for FortiOS 5.6.0 can be purchased in multiples of 100. There is a maximum client limit based on the FortiGate's model. FortiCare enforces the maximum limits when the customer is applying the license to a model.

If you are using the ten free licenses for FortiClient, support is provided on the Fortinet Forum (forum.fortinet.com). Phone support is only available for paid licenses.

Model(s)	Maximum Client Limit
VM00	200
FGT/FWF 30 to 90 series	200
FGT 100 to 400 series	600
FGT 500 to 900 series, VM01, VM02	2,000
FGT 1000 to 2900 series, VM04	50,000
FGT 3700D and above, VM08 and above	100,000

Older FortiClient SKUs will still be valid and can be applied to FortiOS 5.4 and 5.6.

If you are using the ten free licenses for FortiClient, support is provided on the Fortinet Forum (forum.fortinet.com). Phone support is only available for paid licenses.

FortiClient Vulnerability Exemption Setting (407230)

A new CLI command provides a manual override for client computers with vulnerabilities that cannot be fixed.

CLI Syntax

New command to enable/disable compliance exemption for vulnerabilities that cannot be auto patched. Default is `disable`.

```
config endpoint-control profile
   edit <profile-name>
      config forticlient-winmac-setting
         set forticlient-vuln-scan enable
         set forticlient-vuln-scan-exempt [enable|disable]
      end
   next
end
```

DNS profile supports safe search (403275)

Users can take advantage of pre-defined DNS doctor rules to edit DNS profiles and provide safe search for Google, Bing, and YouTube.

To add safe search to a DNS profile - GUI

1. Go to **Security Profiles > DNS Filter**.
2. Edit the default filter or create a new one.
3. Enable **Enforce 'Safe Search on Google, Bing, YouTube**.
4. Select **Strict** or **Moderate** level of restriction for **YouTube Access**.

To add safe search to a DNS profile - CLI

```
config dnsfilter profile
   edit "default"
      set safe-search enable
      set youtube-restrict {strict | moderate} (only available is safe-search enabled)
   next
end
```

Application control and Industrial signatures separate from IPS signatures (382053)

IPS, Application control and industrial signatures have been separated. The get system status command shows the versions of each signature database:

```
get system status
Version: FortiGate-5001D v5.6.0,build1413,170121 (interim)
Virus-DB: 42.00330(2017-01-23 01:16)
Extended DB: 1.00000(2012-10-17 15:46)
Extreme DB: 1.00000(2012-10-17 15:47)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 6.00741(2015-12-01 02:30)
```

Changes to default SSL inspection configuration (380736)

SSL inspection is mandatory in the CLI and GUI and is enabled by default.

GUI Changes

- Updated edit dialogues for IPv4/IPv6 Policy and Explicit Proxy Policy
  - SSL/SSH inspection data displayed in muted palette
  - disabled the toggle button for this option
  - set the default profile as "certificate-inspection"
- Updated list pages for IPv4/IPv6 Policy and Explicit Proxy Policy
  - Add validation for "ssl-ssh-profile" when configuring UTM profiles
- Updated SSL/SSH Inspection list page
  - disabled delete menu on GUI for default ssl profiles
  - changed "Edit" menu to "View" menu for default ssl profiles
  - added implicit class (grayed) the default ssl profile entries
- Updated SSL/SSH Inspection edit dialog
  - disabled all the inputs for default ssl profiles except download/view trusted certificate links
  - changed button to "Return" for default ssl profiles to return the list page
- Updated Profile Group edit dialog
  - removed checkbox for "ssl-ssh-profile" option, make it always required.

CLI changes

1. `ssl-ssh-profile` default value is `certificate-inspection` when applicable in table firewall.profile-group, firewall.policy, firewall.policy6, `firewall.explicit-proxy-policy`

2. make default profiles "certificate-inspection", "deep-ssl-inspection' read only in table firewall.ssl-ssh-profile

Block Google QUIC protocol in default Application Control configuration (385190)

QUIC is an experimental protocol from Google. With recent Google Chrome versions (52 and above), and updated Google services, more than half of connections to Google servers are now in QUIC. This affects the accuracy of Application Control. The default configuration for Application control blocks QUIC.

Users may enable QUIC with CLI commands.

CLI Syntax

```
config application list
   edit <profile-name>
      set options allow-quic
   end
```

Botnet database changes (390756)

Starting in FortiOS 5.6, FortiGate units and FortiGuard Distribution Servers (FDS0 will use object IDs IBDB and DBDB to download and update the Botnet database. Botnet protection will be part of the AntiVirus contract.

FortiOS 5.4 uses object IDs IRDB and BDDB.

Security Fabric audit check for endpoint vulnerability and unauthorized FAP and FSW (401462)

The new Security Fabric Audit feature allows for the display of endpoint vulnerability status in real-time. Users can see:

- FortiClient devices that have critical vulnerabilities detected.
- Discovered FortiSwitches that have not yet been authorized.
- Discovered FortiAPs that have not yet been authorized.

Change to CLI commands for configuring custom Internet services (397029)

Custom internet services are no longer configured through use of the commands `config application internet-service` and `config application internet-service-custom` in the CLI.

These commands are replaced by `config firewall internet-service` and `config firewall internet-service-custom`.

CLI Syntax - examples

```
config firewall internet-service 1245324
   set name "Fortinet-FortiGuard"
   set reputation 5
   set icon-id 140
   set offset 1602565
      config entry
        edit 1
           set protocol 6
           set port 443
           set ip-range-number 27
```

```
            set ip-number 80
         next
         edit 2
            set protocol 6
            set port 8890
            set ip-range-number 27
            set ip-number 80
         next
         edit 3
            set protocol 17
            set port 53
            set ip-range-number 18
            set ip-number 31
         next
         edit 4
            set protocol 17
            set port 8888
            set ip-range-number 18
            set ip-number 31
         next
      end
end



config firewall internet-service-custom
   edit "custom1"
      set comment "custom1"
      config entry
         edit 1
            set protocol 6
            config port-range
               edit 1
                  set start-port 30
                  set end-port 33
               next
            end
            set dst "google-drive" "icloud"
         next
      end
   next
end
```

Enable "sync-session-ttl" in "config ips global" CLI by default (399737)

`sync-session-ttl` is now set to `enable` by default in order to:

- enhance detection of P2P traffic. Efficient detection of P2P is important on hardware accelerated platforms
- ensure that IPS and the kernel use the same ttl
- ensure that IPS sessions time out sooner

CASI functionality moved into application control (385183 372103)

Cloud Access Security Inspection (CASI) is merged with Application Control resulting in changes to the GUI and the CLI.

GUI Changes

- Toggle option added to quickly filter CASI signatures in the Application Signatures list.
- Application Overrides table now shows any parent-child hierarchy using the --parent metadata on signatures. Deleting a parent app also deletes its child apps. And conversely, adding a child app will add all its parent apps but with implicit filter action.
- A policy breakdown is shown on existing application control profiles for policies using the profile. The breakdown indicates which policies are using a deep inspection.
- A breakdown is shown for application categories and filter overrides to indicate the number of CASI and non-CASI signatures. A lock icon is shown for applications requiring deep inspection.

CLI Changes

Commands removed:

- `config application casi profile`
- `casi profile` in `config firewall policy`
- `casi profile` in `config firewall policy6`
- `casi-profile-status` and `casi-profile` under `config firewall sniffer`
- `casi-profile-status` and `casi-profile` under `config firewall interface-policy`

New diagnose command to delete avatars (388634)

Commands to delete avatars by FortiClient UID or avatar name have been added to the CLI.

the two following commands has been added to diagnose endpoint avatar:

- `diagnose endpoint avatar delete <ftcl_uid>`
- `diagnose endpoint avatar delete <ftcl_uid> <username>`

The attribute `delete` did not exist before. The values `<fctl_uid>` and `<user_name>` describe a set of avatars. If only `<fctl_uid>` is defined, all avatars belonging to this FortiClient UID that are not being used will be removed. If both values are defined, the avatar belonging to them will be removed unless they are being used in which case this call will cause an error to user.

Fortinet bar option disabled in profile protocol options when VDOM is in flow-based inspection mode (384953)

In order to prevent the Fortinet Bar from being enabled and redirecting traffic to proxy (WAD) when a VDOM is in flow-based mode, the Fortinet Bar option is disabled in profile protocol options.

SSL/SSH profile certificate handling changes (373835)

In order to support DSA and ECDSA key exchange (in addition to RSA) in SSL resign and replace mode, CLI commands for `deep-inspection` have changed. The `certname` command in `ssl-ssh-profile` has been removed.

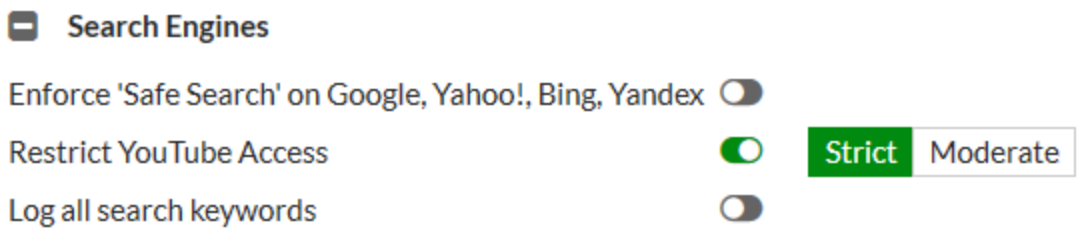
To select from the list of available certificates in the system, use the CLI below.

```
edit deep-inspection
   set server-cert-mode re-sign
   set certname-{rsa | dsa | ecdsa}
```

Restricting access to YouTube (replacement for the YouTube Education filter feature) (378277)

Previous versions of FortiOS supported YouTube for Schools (YTfS). As of July 1, 2016 this feature is no longer supported by YouTube. Instead you can use the information in the YouTube support article Restrict YouTube content on your network or managed devices to achieve the same result. FortiOS supports applying **Strict** or **Moderate** restrictions using HTTP headers as described in this article.

In FortiOS 5.6 with inspection mode set to proxy-based, in a Web Filter profile under **Search Engines** you can select **Restrict YouTube Access** and select either **Strict** or **Moderate**.



Enhancements to IPS Signatures page (285543)

The IPS signatures list page now shows which IPS package is currently deployed. Users can also change their IPS package by linking directly to the FortiGate's **System > FortiGuard** page from the IPS Signatures list page.

DLP sensor GUI changes (307225)

The DLP sensor for file size has been corrected to indicate that the file size has to be greater than the number of KB entered. Previously, the GUI incorrectly showed that the files size could be greater than or equal to the number of KB entered.

Web Filter profile page GUI updates (309012)

The GUI for the **Web Filter** security profile and **Web Profile Overrides** pages are changed.

Web Filter profile page

- removed multilist for override user group and profile
- replaced FortiGuard categories actions icons with font icons
- added tooltip for **Allow users to override blocked categories** to explain the policy group dependency

Web Profile Overrides page

- removed multilist of user, user group, original profile, new profile
- duplicate profile for new profile (for bug #284239)

Web Filter Quota traffic can no longer be set to 0 (374380)

To fix a bug in older major release, the CLI has been changed so that minimum traffic quota does not allow 0 as an entry. The value entered must be in the range of 1 - 4,294,967,295; if 0 is entered, then an error message will be returned.

CLI Commands:

```
config webfilter profile
   edit default
      config ftgd-wf
         config quota
            edit 1
               set type traffic
               set value {a number in the range of 1 - 4,294,967,295}
```

Webcache-https and SSL deep inspection profile configuration changes (381101)

In older releases, the CLI blocked the configuration of the SSL deep inspection profile when webcache-https was enabled. This bug is fixed in FortiOS 5.6.0.

FortiGate conserve mode changes (242562, 386503)

The following changes were made to rework **conserve mode** and facilitate its implementation:

- Implemented CLI commands to configure **extreme**, **red**, and **green** memory usage thresholds in percentages of total RAM. Memory used is the criteria for these thresholds, and set at 95% (extreme), 88% (red) and 82% (green).
- Removed structure av_conserve_mode, other changes in kernel to obtain and set memory usage thresholds from the kernel
- Added conserve mode diagnostic command `diag hardware sysinfo conserve`, which displays information about memory conserve mode.
- Fixed conserve mode logs in the kernel
- Added conserve mode stats to the proxy daemon through command `diag sys proxy stats all | grep conserve_mode`

New custom IPS and Application Control Signatures list (280954)

You can now create IPS and Application control custom signatures by going to **Security Profiles > Custom Signatures**. From here you can create and edit all custom IPS and Application Control signatures.

Server Load balancing

New load balancing features added to FortiOS 5.6.

IPv6, 6to4, and 4to6 server load balancing (280073)

Sever load balancing is supported for:

- IPv6 VIPs (`config firewall vip6`)
- IPv6 to IPv4 (6to4) VIPs (`config firewall vip64`)
- IPv4 to IPv6 (4to6) VIPs (`config firewall vip46`)

Configuration is the same as IPv4 VIPs, except support for advanced HTTP and SSL related features is not available. IPv6 server load balancing supports all the same server types as IPv4 server load balancing (HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL, TCP, UDP, and IP). IPv4 to IPv6 and IPv6 to IPv4 server load balancing supports fewer server types (HTTP, TCP, UDP, and IP).

Improved Server load balancing GUI pages (404169)

Server load balancing GUI pages have been updated and now include more functionality and input verification.

SSL VPN

New SSL VPN features added to FortiOS 5.6.

Remote desktop configuration changes (410648)

If NLA security is chosen when creating an RDP bookmark, a username and password must be provided. However there may be instances where the user might want to use a blank password, despite being highly unrecommended. If a username is provided but the password is empty, the CLI will display a warning. See example CLI below, where the warning appears as a caution before finishing the command:

```
config vpn ssl web user-group-bookmark
   edit <group-name>
      config bookmarks
         edit <bookmark-name>
            set apptype rdp
            set host 172.16.200.121
            set security nla
            set port 3389
            set logon-user <username>
         next
      end
Warning: password is empty. It might fail user authentication and remote desktop
    connection would be failed.
end
```

If no username (`logon-user`) is specified, the following warning message will appear:

```
Please enter user name for RDP security method NLA. object set operator error, -2010
    discard the setting Command fail. Return code -2010
```

SSL VPN supports WAN link load balancing interface (396236)

New CLI command to set `virtual-wan-link` as the destination interface in a firewall policy (when SSL VPN is the source interface) for WAN link load balancing. This allows logging into a FortiGate via SSL VPN for traffic inspection and then have outbound traffic load balanced by WAN link load balancing.

CLI syntax

```
config firewall policy
   edit <example>
      set dstintf virtual-wan-link
end
```

SSL VPN login timeout to support high latency (394583)

With long network latency, the FortiGate can timeout the client before it can finish negotiation processes, such as DNS lookup and time to enter a token. Two new CLI commands under `config vpn ssl settings` have been added that allow the login timeout to be configured, replacing the previous hard timeout value. The second command can be used to set the SSL VPN maximum DTLS hello timeout.

CLI syntax

```
config vpn ssl settings
   edit <example>
      set login-timeout [10-180] Default is 30 seconds.
      set dtls-hello-timeout [10-60] Default is 10 seconds.
end
```

SSL VPN supports Windows 10 OS check (387276)

A new CLI field has been added to the `os-check-list` under `config vpn ssl web portal` to allow OS checking for Windows 10.

CLI syntax

```
config vpn ssl web portal
   edit <example>
   set os-check enable
   config os-check-list windows-10
      set action {deny | allow | check-up-to-date}
   end
end
```

SSL VPN DNS suffix per portal and number of portals (383754)

A new CLI command under `config vpn ssl web portal` to implement a DNS suffix per SSL VPN portal. Each suffix setting for each specific portal will override the `dns-suffix` setting under `config vpn ssl settings`.

This feature also raises bookmark limits and the number of portals that can be supported, depending on what FortiGate series model is used:

- 650 portals on 1000D series
- 1300 portals on 2000E series
- 2600 portals on 3000D series

The previous limit for 1000D series models, for example, was 256 portals.

CLI syntax

```
config vpn ssl web portal
   edit <example>
      set dns-suffix <string>
end
```

New SSL VPN timeout settings (379870)

New SSL VPN timeout settings have been introduced to counter 'Slowloris' and 'R-U-Dead-Yet' vulnerabilities that allow remote attackers to cause a denial of service via partial HTTP requests.

The FortiGate solution is to add two attributes (`http-request-header-timeout` and `http-request-body-timeout`).

CLI syntax

```
config vpn ssl settings
   set http-request-header-timeout [1-60] (seconds)
   set http-request-body-timeout [1-60] (seconds)
end
```

Personal bookmark improvements (377500)

You can now move and clone personal bookmarks in the GUI and CLI.

CLI syntax

```
config vpn ssl web user-bookmark
   edit 'name'
      config bookmarks
      move bookmark1 after/before
      clone bookmark1 to
   next
end
```

New controls for SSL VPN client login limits (376983)

Removed the limitation of SSL VPN user login failure time, by linking SSL VPN user setting with `config user settings` and provided a new option to remove SSL VPN login attempts limitation. New CLI allows the administrator to configure the number of times wrong credentials are allowed before SSL VPN server blocks an IP address, and also how long the block would last.

CLI syntax

```
config vpn ssl settings
   set login-attempt-limit [0-10] Default is 2.
   set login-block-time [0-86400] Default is 60 seconds.
end
```

Unrated category removed from ssl-exempt (356428)

The "Unrated" category has been removed from the SSL Exempt/Web Category list.

Clipboard support for SSL VPN remote desktop connections (307465)

A remote desktop clipboard viewer pane has been added which allows user to copy, interact with and overwrite remote desktop clipboard contents.

System

New system administration features added to FortiOS 5.6.

Remove CLI commands from 1-CPU platforms (405321)

Two CLI commands that set CPU affinity have been removed from 1-CPU platforms since they do not have any impact on these platforms. The commands are `config system global > set miglog-affinity` and `config system global > set av-affinity <string>`.

New SNMP trap for bypass events (307329)

When bypass mode is enabled or disabled on FortiGate units that are equipped with bypass interfaces and support AMC modules, a new SNMP trap is generated and logs bypass events.

Implement SNMP support for NAT Session monitoring which includes new SNMP OIDs (383661)

FortiOS 5.6 implements a new feature providing SNMP support for NAT session monitoring. The resulting new SNMP object identifier (OID) is:

FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgFirewall.fgFwIppools.fgFwIppTables.fgFwIppStatsTable.fgFwIppStatsEntry 1.3.6.1.4.1.12356.101.5.3.2.1.1

Additionally, there are eight new items:

.fgFwIppStatsName .1

.fgFwIppStatsType .2

.fgFwIppStatsStartIp .3

.fgFwIppStatsEndIp .4

.fgFwIppStatsTotalSessions .5

.fgFwIppStatsTcpSessions .6

.fgFwIppStatsUdpSessions .7

.fgFwIppStatsOtherSessions .8

New extended database version OIDs for AV and IPS (402162)

New extended database version OIDs ensure accurate display of the AntiVirus and IPS databases in use when you go to **System > FortiGuard**.

Administrator password encryption hash upgraded from SHA1 to SHA256 (391576)

The encryption has for administrator passwords is upgraded from SHA1 to SHA256.

Downgrades from FortiOS 5.6->5.4->5.2->5.0 will keep the administrator password usable. If you need to downgrade to FortiOS 4.3, remove the password before the downgrade, then login after the downgrade and re-set password.

Allow multiple FortiManager addresses when configuring central management (388083)

Central management configuration can now support multiple FortiManager addresses. This feature is mainly to help the case where the FortiGate unit is behind NAT.

FortiGuard can determine a FortiGate's location from its public IP address (393972)

A new CLI command allows users to determine a FortiGate's location from its public IP address through FortiGuard .

The new CLI command is `diagnose system waninfo`.

Deletion of multiple saved configurations supported (308936)

The FortiGate will save multiple configurations and images when `revision-backup-on-logout` and `revision-image-auto-backup` are enabled in `config system global`.

The deletion of multiple saved configurations is now possible due to changes in the CLI command `execute revision delete config <revision ID>`. Where the command only allowed for one revision ID at a time, it now allows almost ten.

New CLI option to limit script output size (388221)

The new CLI command `set output-size` limits the size of an auto script in megabytes and prevents the memory from being used up by the script's output.

CLI Syntax

```
config system auto-script
   edit <script name>
      set output-size <integer>
   next
end
```

Enter an integer value from 10 to 1024. Default is 10.

Enable / disable logging of SSL connection events (375582)

New CLI commands are added to give the user the option to enable or disable logging of SSL connection events.

CLI Syntax

```
config system global
   set log-ssl-connection {enable | disable}
end
```

Default is `disable`.

Enabling or disabling static key ciphers (379616)

There is a new option in `system global` to enable or disable static key ciphers in SSL/TLS connections (e.g,. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256). The default is enable.

CLI Syntax

```
config system global
   set ssl-static-key-ciphers {enable | disable}
end
```

Enhancements to IPS Signatures page (285543)

The IPS signatures list page now shows which IPS package is currently deployed. You can also change the IPS package by hovering over the information icon next to the IPS package name. Text appears that links directly to the FortiGate's **System > FortiGuard** page from the IPS Signatures list page.

Combine multiple commands into a CLI alias (308921)

You can add one or more CLI command to a CLI alias, then use the `alias` command to run the alias that you have created to execute the stored commands. For example, create the following `alias` to run the `get system status` command:

```
config system alias
   edit "version"
      set command "get system status"
   end
```

Then you can use the following command to run the alias:

```
alias version
```

You can use command abbreviations (for example: `g sys stat` instead of `get system status`). Use quotes around the syntax if there are spaces (there usually are).

You can enter `alias` followed by a ? to view the aliases that you have added.

You can add multiple commands to an alias by pressing **Ctrl-Enter** after the first line. Press enter at the end of subsequent lines. And the end of the last line add second quote and press Enter to end the command.

```
config system alias
   edit "debug_flow"
      set command "diag debug enable
      diag debug flow show console enable"
   end
```

You can include config commands in an alias as well, for example, create the following alias to bring the port1 and port2 interfaces down:

```
config system alias
   edit port12down
      set command "config system interface
      edit port1
      set status down
      next
      edit port2
      set status down
      end"
```

```
    end
```

You can combine `config`, `execute`, `get`, and `diagnose` commands in the same alias, for example:

```
config system alias
   edit "show-info"
      set command "show full-configuration alertemail setting
      get sys status
      dia sys top"
   end
```

VoIP/SIP

This chapter describes new VoIP and SIP features added to FortiOS 5.6.

SIP strict-register enabled by default in VoIP Profiles (380830)

If `strict-register` is disabled, when REGISTER is received by a FortiGate, the source address (usually the IP address of PBX) and ports (usually port 5060) are translated by NAT to the external address of the FortiGate and port 65476. Pinholes are then opened for SIP and RTP. This tells the SIP provider to send incoming SIP traffic to the external address of the FortiGate on port 65476.

This creates a security hole since the port is open regardless of the source IP address so an attacker who scans all the ports by sending REGISTER messages to the external IP of the FortiGate will eventually have one register go through.

When `strict-register` is enabled (the new default) the pinhole is smaller because it will only accept packets from the SIP server.

Enabling `strict-register` can cause problems when the SIP registrar and SIP proxy server are separate entities with separate IP addresses.

SIP diagnose command improvements (376853)

A diagnose command has been added to the CLI that outputs VDOM data located in the voipd daemon.

```
diagnose sys sip-proxy vdom
```

Example

```
(global) # diagnose sys sip-proxy vdom
VDOM list by id:
vdom 0 root (Kernel: root)
vdom 1 dmgmt-vdom (Kernel: dmgmt-vdom)
vdom 2 test2 (Kernel: test2)
vdom 3 test3 (Kernel: test3)
vdom 4 vdoma2 (Kernel: vdoma2)
vdom 5 vdomb2 (Kernel: vdomb2)
vdom 6 vdomc2 (Kernel: vdomc2)
vdom 7 vdoma (Kernel: vdoma)
vdom 8 vdomb (Kernel: vdomb)
vdom 9 vdomc (Kernel: vdomc)
VDOM list by name:
vdom 1 dmgmt-vdom (Kernel: dmgmt-vdom)
```

```
vdom 0 root (Kernel: root)
vdom 2 test2 (Kernel: test2)
vdom 3 test3 (Kernel: test3)
vdom 7 vdoma (Kernel: vdoma)
vdom 4 vdoma2 (Kernel: vdoma2)
vdom 8 vdomb (Kernel: vdomb)
vdom 5 vdomb2 (Kernel: vdomb2)
vdom 9 vdomc (Kernel: vdomc)
vdom 6 vdomc2 (Kernel: vdomc2)
```

WiFi

New WiFi features added to FortiOS 5.6.

Captive Portal Authentication with FortiAP in Bridge Mode (408915)

The FortiGate can operate as a web captive portal server to serve the captive portal local bridge mode.

A new CLI command has been added under `config wireless-controller vap` to set the captive portal type to CMCC, a wireless cipher.

CLI syntax

```
config wireless-controller vap
   edit <name>
      set portal-type { ... | cmcc}
   next
end
```

802.11kv(r) support (405498, 395037)

New CLI commands have been added under `config wireless-controller vap` to set various 802.11kvr settings, or Voice Enterprise (802.11kv) and Fast Basic Service Set (BSS) Transition (802.11r), to provide faster and more intelligent roaming for the client.

CLI syntax

```
config wireless-controller vap
   edit <name>
      set voice-enterprise {enable | disable}
      set fast-bss-transition {enable | disable}
      set ft-mobility-domain
      set ft-r0-key-lifetime [1-65535]
      set ft-over-ds {enable | disable}
   next
end
```

External Captive Portal authentication with FortiAP in Bridge Mode (403115, 384872)

New CLI commands have been added under `config wireless-controller vap` to set various options for external captive portal with FortiAP in Bridge Mode. The commands set the standalone captive portal server category, the server's domain name or IP address, secret key to access the RADIUS server, and the standalone captive portal Access Controller (AC) name.

Note that these commands are only available when **local-standalone** is set to **enable** and **security** is set to **captive-portal**.

CLI syntax

```
config wireless-controller vap
   edit <name>
```

```
      set captive-portal-category {FortiCloud | CMCC} Default is FortiCloud.
      set captive-portal-radius-server <server>
      set captive-portal-radius-secret <password>
      set captive-portal-ac-name <name>
   next
end
```

Japan DFS support for FAP-421E/423E/S421E/S423E (402287, 401434)

Korea and Japan Dynamic Frequency Selection (DFS) certification has been added for FAP-421E/423E/S421E/S423E. DFS is a mechanism that allows WLANs to select a frequency that does not interfere with certain radar systems while operating in the 5 GHz band.

802.3az support on WAVE2 WiFi APs (400558)

A new CLI command has been added under `config wireless-controller wtp-profile` to enable or disable use of Energy-Efficient Ethernet (EEE) on WTP, allowing for less power consumption during periods of low data activity.

CLI syntax

```
config wireless-controller wtp-profile
   edit <profile-name>
      set energy-efficient-ethernet {enable|disable}
end
```

CLI command update made in wids-profile (400263)

The CLI command `rogue-scan` under `config wireless-controller wids-profile` has been changed to `sensor-mode` and allows easier configuration of radio sensor mode. Note that while `foreign` enables radio sensor mode on foreign channels only, `both` enables the feature on foreign and home channels.

CLI syntax

```
config wireless-controller wids-profile
   edit <example>
      set sensor-mode {disable|foreign|both}
end
```

Channel utilization, FortiPresence support on AP mode, QoS enhancement for voice (399134, 377562)

A new CLI command has been added, `config wireless-controller qos-profile`, to configure quality of service (QoS) profiles where you can add WiFi multi-media (WMM) control and Differentiated Services Code Point (DSCP) mapping.

Note that:

- `call-capacity` and `bandwidth-admission-control` are only available when `call-admission-control` is set to `enable`.
- `bandwidth-capacity` is only available when `bandwidth-admission-control` is set to `enable`.
- All DSCP mapping options are only available when `dscp-wmm-mapping` is set to `enable`.

- wmm is already set to enable by default. If wmm is set to disable, the following entries are *not* available: wmm-uapsd, call-admission-control, and dscp-wmm-mapping.

CLI syntax

```
config wireless-controller qos-profile
   edit <example>
      set comment <comment>
      set uplink [0-2097152] Default is 0 Kbps.
      set downlink [0-2097152] Default is 0 Kbps.
      set uplink-sta [0-2097152] Default is 0 Kbps.
      set downlink-sta [0-2097152] Default is 0 Kbps.
      set burst {enable|disable} Default is disable.
      set wmm {enable|disable} Default is enable.
      set wmm-uapsd {enable|disable} Default is enable.
      set call-admission-control {enable|disable} Default is disable.
      set call-capacity [0-60] Default is 10 phones.
      set bandwidth-admission-control {enable|disable} Default is disable.
      set bandwidth-capacity [1-600000] Default is 2000 Kbps.
      set dscp-wmm-mapping {enable|disable} Default is disable.
      set dscp-wmm-vo [0-63] Default is 48 56.
      set dscp-wmm-vi [0-63] Default is 32 40.
      set dscp-wmm-be [0-63] Default is 0 24.
      set dscp-wmm-bk [0-63] Default is 8 16.
```

QoS profiles can be assigned under the config wireless-controller vap command using qos-profile.

FortiCloud managed APs can now be applied a bandwidth restriction or rate limitation based on SSID. For instance if guest and employee SSIDs are available, you can rate limit guest access to a certain rate to accommodate for employees. This feature also applies a rate limit based on the application in use, as APs are application aware.

FAP-U421E and FAP-U423E support (397900)

Two Universal FortiAP models support FortiOS 5.6. Their default profiles are added under config wireless-controller wtp-profiles, as shown below:

CLI syntax

```
config wireless-controller wtp-profile
   edit "FAPU421E-default"
      config platform
         set type U421E
      end
      set ap-country US
      config radio-1
         set band 802.11n
      end
      config radio-2
         set band 802.11ac
      end
   next
end

config wireless-controller wtp-profile
```

```
    edit "FAPU423E-default"
       config platform
          set type U423E
       end
       set ap-country US
       config radio-1
          set band 802.11n
       end
       config radio-2
          set band 802.11ac
       end
    next
end
```

Minor reorganization of WiFi GUI entries (396497)

WiFi & Switch Controller GUI entries **Managed FortiAPs**, **SSID**, **FortiAP Profiles**, and **WIDS Profiles** have been reorganized.

Multiple PSK support for WPA personal (393320, 264744)

New CLI commands have been added, under `config wireless-controller vap`, to configure multiple WiFi Protected Access Pre-Shared Keys (WPA-PSKs), as PSK is more secure without all devices having to share the same PSK.

Note that, for the following multiple PSK related commands to become available, `vdom`, `ssid`, and `passphrase` all have to be set first.

CLI syntax

```
config wireless-controller vap
   edit <example>
      set mpsk {enable|disable}
      set mpsk-concurrent-clients [0-65535] Default is 0.
      config mpsk-key
         edit key-name <example>
            set passphrase <wpa-psk>
            set concurrent-clients [0-65535] Default is empty.
            set comment <comments>
         next
      end
end
```

Use the `mpsk-concurrent-clients` entry to set the maximum number of concurrent connected clients for each `mpsk` entry. Use the `mpsk-key` configuration method to configure multiple `mpsk` entries.

Table size of qos-profile has VDOM limit (388070)

The command `config wireless-controller qos-profile` now has VDOM table limit; there is no longer an unlimited number of entries within each VDOM.

Add "dhcp-lease-time" setting to local-standalone-nat VAP (384229)

When a Virtual Access Point (VAP) has been configured for a FortiAP, a DHCP server is automatically configured on the FortiAP side with a hard lease time. A new CLI command under `config wireless-controller vap` has been added to customize the DHCP lease time for NAT IP address. This is to solve issues where the DHCP IP pool was exhausted when the number of clients grew too large for the lease time span.

Note that the new command, `dhcp-lease-time`, is only available when `local-standalone` is set to `enable`, then setting `local-standalone-nat` to `enable`.

CLI syntax

```
config wireless-controller vap
   edit <example>
      set local-standalone {enable|disable}
      set local-standalone-nat {enable|disable}
      set dhcp-lease-time [300-8640000] Default is 2400 seconds.
end
```

New CLI command to configure LDPC for FortiAP (383864)

Previously, LDPC value on FortiAP could only be changed on FortiAP local CLI. Syntax has been added in FortiOS CLI under the 'wireless-controller.vap' entry to configure the LDPC value on FortiAP.

CLI Syntax

```
configure wireless-controller vap
   edit 1
      set ldpc [enable|rx|tx|disable]
end
```

New region code/SKU for Indonesia (382926)

A new country region code, F, has been added to meet Indonesia's WiFi channel requirements. Indonesia previously belonged to region code W.

FortiAP RMA support added (381936)

New CLI command `fortiap` added under `exe replace-device` to replace an old FortiAP's serial number with a new one.

CLI Syntax

```
execute replace-device fortiap <old-fortiap-id> <new-fortiap-id>
```

Support fixed-length 64-hex digit for WPA-Personal passphrase (381030)

WPA-Personal passphrase now supports a fixed-length of 64 hexadecimal digits.

Allow FortiGates to manage cloud-based FortiAPs (380150)

FortiGates can now manage cloud-based FortiAPs using the new `fapc-compatibility` command under `wireless-controller setting`.

If enabled, default FAP-C wtp-profiles will be added. If disabled, FAP-C related CMDB configurations will be removed: wtp-group in vap's vlan-pool, wtp-group, ws, wtp, wtp-profile.

CLI syntax

```
config wireless-controller setting
   set country CN
   set fapc-compatibility [enable|disable]
end
```

You will receive an error message when trying to change `country` while `fapc-compatibility` is enabled. You need to disable `fapc-compatibility` before changing to an FAPC unsupported country.

Use IPsec instead of DTLS to protect CAPWAP tunnels (379502)

This feature is to utilize FortiAP hardware to improve the throughput of tunneled data traffic by using IPsec when data security is enabled.

"AES-256-CBC & SHA256" algorithm and "dh_group 15" are used for both CAPWAP IPsec phase1 and phase 2.

FAP320B will not support this feature due to its limited capacity of free flash.

New option added to support only one IP per one endpoint association (378207)

When users change configuration, the radiusd will reset all configurations and refresh all logons in the kernel. All these actions are done in the one loop. A CLI option has been added to enable/disable replacement of an old IP address with a new IP address for the same endpoint on RADIUS accounting start.

CLI Syntax

```
configure user radius
   edit radius-root
      set rsso-ep-one-ip-only [enable|disable]
   next
end
```

FAP-222C-K DFS support (377795)

Dynamic Frequency Selection (DFS) bands can now be configured for FortiAP 222C-K.

Note that this FortiAP model has the Korean region code (K), but `ap-country` under `config wireless-controller wtp-profile` still needs to be set to `KR`.

CLI syntax

```
config wireless-controller wtp-profile
```

```
    edit <K-FAP222C>
       config platform
          set type <222C>
       end
       set ap-country KR
       config radio-2
          set band <802.11ac>
          set vap-all <disable>
          set vaps "vap-vd-07"
          set channel "52" "56" "60" "64" "100" "104" "108" "112" "116" "120" "124" "128"
              "132" "136" "140"
       end
    next
end
```

Dynamic VLAN support in standalone mode (377298)

Dynamic VLAN is now supported in standalone mode. Previously, dynamic VLAN only worked in local bridge mode.

CLI-only features added to GUI (376891)

Previously CLI-only features have been added to the GUI under **FortiAP Profiles**, **Managed FortiAPs**, and **SSID**. Also fixed issue where the correct value is displayed when viewing the **WIDS Profile** notification icon under **FortiAP Profiles**.

Managed AP GUI update (375376)

Upgraded Managed FortiAPs dialog page to a newer style, including icons for SSID and LAN port.

Bonjour gateway support (373659)

Bonjour gateway now supported for WiFi networks.

Syntax

```
config wireless-controller bonjour-profile
   edit 0
      set comment "comment"
      config policy-list
         edit 1
            set description "description"
            set from-vlan [0-4094] Default is 0.
            set to-vlan [0-4094|all] Default is all.
            set services [all|airplay|afp|bit-
                torrent|ftp|ichat|itunes|printers|samba|scanners|ssh|chromecast]
         next
      end
   next
end
```

FAP421E/423E wave2 support (371374)

Previously removed wave2 FAP421E and FAP423E models have been reinstated and are now supported again. The models are available again through the CLI and GUI. These models are listed under the **Platform** dropdown menu when creating a new FortiAP Profile under **WiFi & Switch Controller > FortiAP Profiles**.

CLI syntax

```
config wireless-controller wtp-profile
   edit <example>
   config platform
      set type <...|421E|423E>
   end
end
```

WiFi Health Monitor GUI changes (308317)

The Wifi Health Monitor page has been improved, including the following changes:

- Flowchart used for diagrams
- Chart used for interference and AP clients
- Removed spectrum analysis
- Added functionality to upgrade FortiAP firmware
- Added option to view both 2.4GHz and 5GHz data simultaneously

AP Profile GUI page updates (298266)

The AP Profile GUI page has been upgraded to a new style including AngularJS code.

N+1 Wireless Controller HA (294656)

Instances of failover between FortiAP units was too long and lead to extended periods of time where WiFi users were without network connection. Because WiFi is considered a primary network connection in today's verticals (including enterprise, retail, education, warehousing, healthcare, government, and more), it is necessary for successful failover to occur as fast as possible.

You can now define the role of the primary and secondary controllers on the FortiAP unit, allowing the unit to decide the order in which the FortiAP selects the FortiGate. This process was previously decided on load-based detection, but can now be defined by each unit's pre-determined priority. In addition, heartbeat intervals have been lowered to further improve FortiAP awareness and successful failover.

Syntax

```
config wireless-controller inter-controller
   set inter-controller-mode {disable | l2-roaming | 1+1} Default is disable.
   set inter-controller-key <password>
   set inter-controller-pri {primary | secondary} Default is primary.
   set fast-failover-max [3-64] Default is 10.
   set fast-failover-wait [10-86400] Default is 10.
   config inter-controller-peer
      edit <name>
```

```
            set peer-ip <ip-address>
            set peer-port [1024-49150] Default is 5246.
            set peer-priority {primary | secondary} Default is primary.
        next
    end
end
```

Support for duplicate SSID names on tunnel and bridge mode interfaces (278955)

When `duplicate-ssid` is enabled in the CLI, this feature allows VAPs to use the same SSID name in the same VDOM. When disabled, all SSIDs in WLAN interface will be checked—if duplicate SSIDs exist, an error message will be displayed. When `duplicate-ssid` is enabled in the CLI, duplicate SSID check is removed in "Edit SSID" GUI page.

Syntax

```
config wireless-controller setting
   set duplicate-ssid [enable|disable]
   next
end
```

Controlled failover between wireless controllers (249515)

Instances of failover between FortiAP units was too long and lead to extended periods of time where WiFi users were without network connection. Because WiFi is considered a primary network connection in today's verticals (including enterprise, retail, education, warehousing, healthcare, government, and more), it is necessary for successful failover to occur as fast as possible.

Administrators can now define the role of the primary and secondary controllers on the FortiAP unit, allowing the unit to decide the order in which the FortiAP selects the FortiGate. This process was decided on load-based detection, but can now be defined by each unit's pre-determined priority. In addition, heartbeat intervals have been lowered to further improve FortiAP awareness and successful failover.

FORTINET

High Performance Network Security

Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.